TREND MICRO™

OfficeScan™ 10.6

For Enterprise and Medium Business

SP1 Manuel de l'administrateur

Sécurité des points finaux

Protection en ligne

Sécurité Web

Trend Micro Incorporated se réserve le droit de modifier sans préavis ce document et les produits décrits dans ce document. Avant d'installer et d'utiliser votre logiciel, veuillez consulter les fichiers Lisez-moi, les notes de mise à jour et la dernière version de la documentation utilisateur applicable que vous trouverez sur le site Web de Trend Micro à l'adresse suivante:

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Trend Micro, le logo t-ball de Trend Micro, OfficeScan, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect, et TrendLabs sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Copyright © 1998-2012 Trend Micro Incorporated. Tous droits réservés.

Nº de référence du document : OSEM105375_120409

Date de publication : mai 2012

Protégé par les brevets américains n° 5,623,600; 5,889,943; 5,951,698 et 6,119,165

La documentation utilisateur pour Trend Micro OfficeScan présente les fonctions principales du logiciel et les instructions d'installation pour votre environnement de production. Lisez attentivement ce manuel avant d'installer ou d'utiliser le logiciel.

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du logiciel dans le fichier d'aide en ligne et dans la Base de connaissances en ligne sur le site Web de Trend Micro.

Trend Micro cherche toujours à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Veuillez évaluer cette documentation sur le site Web suivant :

http://www.trendmicro.com/download/documentation/rating.asp

Table des matières

Préface

Préface 1

Documentation OfficeScan 2

Public cible 3

Conventions typographiques du document 3

Terminologie 4

Chapitre 1: Présentation d'OfficeScan

À propos d'OfficeScan 1-2

Nouveautés de cette version 1-2

- Gestion des stratégies depuis Control Manager 1-2
- Compatibilité de la surveillance des comportements avec une architecture 64 bits 1-3
- Compatibilité de l'autoprotection client avec une architecture 64 bits 1-3
- Compatibilité du contrôle des dispositifs avec une architecture 64 bits lors de la prévention des modifications non autorisées 1-3
- Améliorations apportées à la protection des données 1-4
- Améliorations de Virtual Desktop Infrastructure 1-4
- Scan étendu des ports dans le cadre des stratégies de réputation des sites Web 1-4
- Nouveautés de la version 10.6 1-5

Fonctionnalités et avantages principaux 1-9

Le serveur OfficeScan 1-12

Le client OfficeScan 1-13

Intégration aux produits et services de Trend Micro 1-14

Chapitre 2: Démarrage d'OfficeScan

La console Web 2-2
Configuration requise pour l'ouverture de la console Web 2-2
Compte de connexion 2-3
La bannière de la console Web 2-4

Le tableau de bord récapitulatif 2-5
Section de l'état de la licence de produit 2-6
Onglets et widgets 2-7

Intégration d'Active Directory 2-27
Intégration d'Active Directory dans OfficeScan 2-28
Synchronisation des données avec les domaines Active Directory 2-30

L'arborescence des clients OfficeScan 2-31
Tâches générales dans l'arborescence des clients 2-32
Tâches spécifiques dans l'arborescence des clients 2-35

Domaines OfficeScan 2-44
Regroupement des clients 2-45

Chapitre 3: Utilisation de Trend Micro Smart Protection

À propos de Trend Micro Smart Protection 3-2
Le besoin d'une nouvelle solution 3-2

Services Smart Protection 3-3
Services de File Reputation 3-3
Services de réputation de sites Web 3-4
Smart Feedback 3-5

Sources Smart Protection 3-6
Trend Micro Smart Protection Network 3-6
Smart Protection Server 3-7
Sources Smart Protection comparées 3-7

Fichiers de signatures Smart Protection 3-8
Smart Scan Agent Pattern 3-8
Smart Scan Pattern 3-9
Liste de blocage de sites Web 3-9
Processus de mise à jour des signatures Smart Protection 3-10
Utilisation des signatures Smart Protection 3-11

Configuration des services Smart Protection 3-13
Installation du serveur Smart Protection Server 3-14
Gestion du serveur Smart Protection Server intégré 3-19
Liste des sources Smart Protection 3-23
Paramètres du proxy de la connexion du client 3-30
Paramètres d'emplacement de l'ordinateur 3-31
Installations de Trend Micro Network VirusWall 3-31

Utilisation des services Smart Protection 3-31

Chapitre 4: Installation du client OfficeScan

Installations récentes du client OfficeScan 4-2

Remarques relatives à l'installation 4-2
Fonctionnalités du client OfficeScan 4-3
Installation du client OfficeScan et prise en charge d'IPv6 4-7

Éléments à prendre en compte pour le déploiement 4-10
Installations de la page Web d'installation 4-14
Installation basée sur le navigateur 4-16
Exécution d'une installation basée sur UNC 4-17
Installation à distance depuis OfficeScan Web Console 4-18
Installation avec l'outil Configuration du script de connexion 4-20
Installation avec Client Packager 4-23
Installations à partir d'une image disque client 4-36
Utilisation de Vulnerability Scanner 4-37
Installation avec la conformité à la sécurité 4-61

Migration vers le client OfficeScan 4-63
Migration à partir d'autres logiciels de sécurité de points finaux .. 4-63
Migration depuis des serveurs ServerProtect Normal 4-64

Tâches après l'installation 4-67
Raccourci du client OfficeScan 4-68
Liste des programmes 4-68
Services du client OfficeScan 4-68
Journaux d'installation du client OfficeScan 4-69
Tâches recommandées après l'installation 4-69

Désintallation du client OfficeScan 4-70
Désinstallation du client OfficeScan de la console Web 4-71

Le programme de désinstallation du client OfficeScan 4-72
Désinstallation manuelle du client OfficeScan. 4-73

Chapitre 5: Maintien d'une protection à jour

Composants et programmes OfficeScan 5-2
Composants de l'antivirus 5-2
Composants de Damage Cleanup Services 5-6
Composants du service Anti-spyware 5-6
Composants du pare-feu 5-7
Composant lié à la réputation de sites Web 5-8
Composants de surveillance des comportements 5-8
Programmes 5-9

Présentation de la mise à jour 5-12
Mise à jour du serveur OfficeScan et client OfficeScan 5-12
Mise à jour des sources Smart Protection 5-14

Mises à jour du serveur OfficeScan 5-15
Sources de mise à jour du serveur OfficeScan 5-17
Proxy pour les mises à jour du serveur OfficeScan 5-18
Configuration de la source de mise à jour du serveur 5-19
Duplication des composants du serveur OfficeScan 5-20
Mises à jour de serveur OfficeScan isolé 5-23
Méthodes de mise à jour du serveur OfficeScan 5-25
Journaux de mise à jour du serveur OfficeScan 5-26

Mises à jour du serveur Smart Protection Server intégré 5-27

Mise à jour des clients OfficeScan 5-27
Sources de mise à jour des clients OfficeScan 5-29
Méthodes de mise à jour du client OfficeScan 5-37
Configuration de l'espace disque réservé pour les mises à jour clients OfficeScan 5-49
Proxy pour la mise à jour des composants du client OfficeScan .. 5-49
Configuration des notifications de mise à jour du client OfficeScan 5-51
Affichage des journaux de mise à jour du client OfficeScan 5-52
Applicatios des mises à jour du client OfficeScan 5-53
Rétrogadation des composants pour les clients OfficeScan 5-53

Exécution de l'outil Touch Tool pour les correctifs de type Hot Fix des clients OfficeScan 5-54

Agents de mise à jour 5-55
Configuration minimale requise pour les agents de mise à jour ... 5-56
Configuration de l'agent de mise à jour 5-56
Sources de mises à jour pour les agents de mises à jour 5-58
Méthodes de mise à jour pour les agents de mise à jour 5-63
Rapport d'analyse de l'agent de mise à jour 5-63

Résumé des mises à jour de composants 5-64
État de mise à jour des clients OfficeScan 5-65
Composants 5-65

Chapitre 6: Recherche des risques de sécurité

À propos des risques de sécurité 6-2
Virus et programmes malveillants 6-2
Spywares et graywares 6-4

Méthodes de scan 6-8
Méthode de scan par défaut 6-8
Comparaison des méthodes de scan 6-9
Changement de la méthode de scan 6-9
Passage de Smart Scan au scan traditionnel 6-10
Passage du scan traditionnel à Smart Scan 6-11

Types de scan 6-14
Scan en temps réel 6-15
Scan manuel 6-18
Scan programmé 6-20
Scan immédiat 6-23

Paramètres communs à tous les types de scan 6-27
Critères de scan 6-27
Exclusions de scan 6-31
Actions de scan 6-36
Restauration des fichiers chiffrés 6-44
Actions de scan anti-spywares/graywares 6-48
Liste des spywares/graywares approuvés 6-49
Restauration des spywares/graywares 6-51

Privilèges et autres paramètres de scan 6-52
Privilèges de type de scan 6-53
Privilèges et autres paramètres de scan programmé 6-56
Privilèges et autres paramètres du scan de courrier 6-62
Paramètres du cache pour les scans 6-65

Paramètres de scan généraux 6-69
Configuration des paramètres de scan généraux 6-69
Section des paramètres de scan 6-70
Section des paramètres de scan programmé 6-76
Section des paramètres de bande passante des journaux de virus/programmes malveillants 6-78

Notifications sur les risques liés à la sécurité 6-79
Notifications sur les risques liés à la sécurité pour les administrateurs 6-79
Notifications sur les risques liés à la sécurité pour les utilisateurs du client OfficeScan 6-83
Notification de redémarrage destinée aux clients afin de terminer le nettoyage des fichiers infectés 6-86

Journaux de risques de sécurité 6-87
Affichage des journaux de virus/programmes malveillants 6-87
Affichage des journaux de spywares/graywares 6-94
Journaux de scan 6-97

Épidémies de risques liés à la sécurité 6-98
Critères et notifications d'épidémies de risques liés à la sécurité .. 6-99
Configuration de la prévention des épidémies de risques liés à la sécurité 6-103
Stratégies de prévention des épidémies 6-104
Désactivation de la prévention des épidémies 6-108

Chapitre 7: Utilisation de la surveillance des comportements

Surveillance des comportements 7-2
Blocage du comportement des programmes malveillants 7-2
Surveillance des événements 7-3
Liste d'exceptions de la surveillance des comportements 7-6

Privilèges de surveillance des comportements 7-10
Autorisation de privilèges de surveillance des comportements 7-11

Notifications de surveillance des comportements pour les utilisateurs du client OfficeScan 7-11
Activation de l'envoi de messages de notification 7-12
Modification du contenu du message de notification 7-12

Journaux de surveillance des comportements 7-13
Affichage des journaux de surveillance des comportements 7-13
Configuration de la programmation d'envoi de journaux de surveillance des comportements 7-14

Chapitre 8: Utilisation du contrôle des dispositifs

Contrôle des dispositifs 8-2
Autorisations pour les périphériques de stockage 8-3
Autorisations pour les périphériques qui ne sont pas destinés au stockage 8-10

Modification des notifications du contrôle des dispositifs 8-17

Journaux de contrôle des dispositifs 8-17
Affichage des journaux de contrôle des dispositifs 8-18

Chapitre 9: Gestion de la protection des données et mise en œuvre de la prévention contre la perte de données

Installation de la protection des données 9-2
Installation de la protection des données 9-3

Licence de protection des données 9-4
Activation ou renouvellement de la licence de protection des données. 9-4
Affichage des informations de licence de protection des données 9-5

Déploiement de la protection des données vers les clients 9-6
Déploiement du module Protection des données sur des Clients .. 9-7

À propos de la prévention contre la perte de données 9-9

Stratégies de prévention contre la perte de données 9-11
Configuration de la stratégie 9-12

Types d'identificateurs de données 9-13
Modèles de prévention contre la perte de données 9-27
Canaux DLP 9-32
Mesures de prévention contre la perte de données 9-45
Configuration de la stratégie de prévention contre la perte de données 9-50
Outil Liste de dispositifs 9-54

Notifications de la prévention contre la perte de données 9-55
Notifications de la prévention contre la perte de données pour les administrateurs 9-56
Notifications de prévention contre la perte de données pour les utilisateurs clients 9-59

Journaux de prévention contre la perte de données 9-60
Affichage des journaux de prévention contre la perte de données 9-60
Journaux de débogage de protection des données 9-65

Désinstallation de la protection des données 9-66
Désinstallez la protection de données à partir de Plug-In Manager 9-67

Chapitre 10: Protection des ordinateurs contre les menaces Internet

À propos des menaces Internet 10-2

Réputation de sites Web 10-2

Stratégies de réputation de sites Web 10-3
Configuration de Stratégie de réputation de sites Web 10-3

Proxy pour l'évaluation de la réputation de sites Web 10-9

Notifications sur les menaces Internet pour les utilisateurs clients 10-10
Activation des messages de notification sur les menaces Internet 10-10
Modification des messages de notification sur les menaces Internet 10-11

Journaux de réputation de sites Web 10-11
Affichage de journaux de réputation de sites Web 10-11

Chapitre 11: Utilisation du pare-feu OfficeScan

À propos du pare-feu OfficeScan 11-2
- Filtrage du trafic 11-2
- Filtrage d'applications 11-3
- Liste Certified Safe Software 11-3
- Recherche de virus de réseau 11-3
- Profils et stratégies personnalisables 11-4
- Stateful Inspection 11-4
- Système de détection d'intrusion 11-4
- Surveillance des épidémies de violation de pare-feu 11-6
- Privilèges du pare-feu clients OfficeScan 11-6

Activation ou désactivation du pare-feu OfficeScan 11-6
- Activation ou désactivation du pare-feu OfficeScan sur les ordinateurs sélectionnés 11-7
- Activation ou désactivation du pare-feu OfficeScan sur tous les ordinateurs 11-8

Stratégies et profils de pare-feu 11-8
- Stratégies de pare-feu 11-9
- Profils de pare-feu 11-18

Privilèges du pare-feu 11-24
- Accord des privilèges de pare-feu 11-26

Paramètres généraux du pare-feu 11-27
- Configuration des paramètres généraux de pare-feu 11-28

Notifications de violation du pare-feu pour les utilisateurs clients OfficeScan 11-28
- Accorder aux utilisateurs le privilège d'activer/désactiver le message de notification 11-29
- Modification du contenu du message de notification de pare-feu 11-30

Journaux de pare-feu 11-30
- Affichage des journaux du pare-feu 11-31

Épidémies de violation du pare-feu 11-32
- Configuration des critères et notifications de l'épidémie de violation du pare-feu 11-32

Test du pare-feu OfficeScan 11-34

Chapitre 12: Gestion du serveur OfficeScan

Administration basée sur les rôles 12-2
Rôles utilisateurs 12-3
Rôles utilisateurs intégrés 12-11
Rôles personnalisés 12-12
Comptes utilisateurs 12-19

Trend Micro Control Manager 12-24
Intégration de Control Manager dans cette version d'OfficeScan 12-25
Versions de Control Manager prises en charge 12-27
Enregistrement d'OfficeScan sur Control Manager 12-28
Vérification de l'état d'OfficeScan sur la console d'administration de Control Manager 12-29

Serveurs de référence 12-30
Gestion de la liste de serveurs de référence 12-31

Paramètres de notification aux administrateurs 12-32
Configuration des paramètres de notifications aux administrateurs 12-33

Journaux des événements du système 12-35
Affichage des journaux d'évènements du système 12-35

Gestion du journal 12-36
Maintenance des journaux 12-37

Licences 12-40
Affichage des informations sur la licence produit 12-41
Activation ou renouvellement d'une licence 12-42

Sauvegarde de la base de données d'OfficeScan 12-43
Sauvegarde de la base de données OfficeScan 12-43
Restauration des fichiers de sauvegarde de la base de données .. 12-44

Informations relatives au serveur Web OfficeScan 12-45
Configuration des paramètres de connexion 12-45

Mot de passe de la console Web 12-46

Paramètres de la console Web 12-46
Configuration des paramètres de la console Web 12-46

Gestionnaire de quarantaine 12-47
Configuration des paramètres du répertoire de quarantaine 12-47
Server Tuner 12-48
Exécution du Server Tuner 12-49
Smart Feedback 12-51
Participation au programme Smart Feedback 12-52

Chapitre 13: Gestion du client OfficeScan

Emplacement de l'ordinateur 13-2
Critères d'emplacement 13-3
Configuration des paramètres d'emplacement 13-3
Gateway Settings Importer 13-5
Gestion des programmes du client OfficeScan 13-6
Services du client OfficeScan 13-7
Redémarrage des services du client OfficeScan 13-12
Autoprotection client 13-13
Sécurité du client OfficeScan 13-17
Restriction de l'accès à la console client OfficeScan 13-18
Déchargement du client OfficeScan 13-19
Privilège des clients OfficeScan itinérants 13-20
Client Mover 13-23
Clients OfficeScan inactifs 13-25
Connexion client-serveur 13-26
Icônes du client OfficeScan 13-26
Vérification de la connexion client-serveur 13-43
Journaux de vérification de la connexion 13-44
Clients inaccessibles 13-45
Paramètres proxy du client OfficeScan 13-50
Proxy interne pour les clients OfficeScan 13-50
Proxy externe pour les clients OfficeScan 13-51
Privilèges de configuration proxy pour les clients 13-52
Paramètres proxy automatique pour le client OfficeScan 13-53
Affichage des informations du client OfficeScan 13-55
Importation et exportation des paramètres du client 13-55
Exportation des paramètres du client 13-56

Importation des paramètres du client 13-56

Conformité de la sécurité 13-57
Conformité de la sécurité pour les clients gérés 13-58
Rapports de conformité à la demande 13-67
Rapports de conformité planifiés 13-70
Conformité de la sécurité pour les points finaux non gérés 13-71

Trend Micro Virtual Desktop Support 13-76
Installation de Virtual Desktop Support 13-77
Licence de Virtual Desktop Support 13-79
Connexions Virtual Server 13-81
Dépannage des connexions Microsoft Hyper-V 13-83
Outil de génération de modèle de pré-scan VDI 13-86

Paramètres clients généraux 13-89

Configuration des privilèges clients et autres paramètres 13-90

Chapitre 14: Utilisation de Plug-In Manager

À propos de Plug-In Manager 14-2
Agents côté client et Plug-in Manager client 14-3
Widgets 14-3

Installation de Plug-In Manager 14-3
Exécution de tâches après l'installation 14-4

Gestion des fonctionnalités natives d'OfficeScan 14-4

Gestion des plugiciels 14-4
Installation de plug-ins 14-5
Gestion des plug-ins 14-6
Mises à niveau de plug-ins 14-7
Désinstallation de plug-ins 14-8

Désinstallation de Plug-In Manager 14-9

Dépannage de Plug-In Manager 14-10
Un plugiciel ne s'affiche pas dans la console de Plug-in Manager 14-10
Problèmes d'installation et d'affichage côté client de l'agent 14-11
Cette version du serveur Web Apache n'est pas prise en charge 14-12

Un agent côté client ne peut pas être lancé si la configuration du script de configuration automatique dans Internet Explorer redirige vers un serveur proxy 14-13
Une erreur s'est produite dans le système, le module de mise à jour ou le programme Plug-in Manager et le message d'erreur fournit un certain code d'erreur 14-15

Chapitre 15: Utilisation de Policy Server pour Cisco NAC

À propos de Policy Server pour Cisco NAC 15-3
Composants et terminologie 15-3
Composants 15-3
Terminologie 15-5
Architecture Cisco NAC 15-7
Séquence de validation du client 15-8
Serveur Policy Server 15-10
Stratégies et règles du serveur Policy Server 15-11
Synchronisation 15-18
Certificats 15-19
Configuration minimale requise pour le serveur Policy Server 15-22
Configuration requise pour Cisco Trust Agent (CTA) 15-23
Plates-formes prises en charge et configuration requise 15-24
Déploiement de Policy Server for NAC 15-25
Inscription du serveur Cisco Secure ACS 15-27
Installation du certificat CA 15-27
Déploiement de Cisco Trust Agent 15-30
Installation du serveur Policy Server for Cisco NAC 15-35
Préparation du certificat SSL du serveur Policy Server 15-38
Configuration du serveur ACS 15-41
Configuration du serveur Policy Server for Cisco NAC 15-42

Chapitre 16: Configuration d'OfficeScan avec des logiciels tiers

Aperçu général de l'architecture et de la configuration de Check Point 16-2
Intégration d'OfficeScan 16-3
Configuration du fichier Secure Configuration Verification pour OfficeScan 16-4
Installation du support SecureClient 16-6
Accord de privilège d'affichage de l'onglet Boîte à outils pour les utilisateurs 16-7
Installation du support SecureClient 16-8

Chapitre 17: Obtenir de l'aide

Ressources de dépannage 17-2
Support Intelligence System 17-2
Case Diagnostic Tool 17-2
Trend Micro Performance Tuning Tool 17-2
Journaux du serveur OfficeScan 17-3
Journaux du client OfficeScan 17-15
Comment contacter l?assistance technique 17-24
Contact 17-24
Optimisation de votre demande d'assistance 17-25
Base de connaissances Trend Micro 17-25
Centre d'informations de sécurité 17-26
Envoi de fichiers suspects à Trend Micro 17-27
Commentaires relatifs à la documentation 17-27

Annexe A: Prise en charge de l'adressage IPv6 dans OfficeScan

Prise en charge de l'adressage IPv6 pour les serveurs et les clients OfficeScan. A-2
Configuration requise pour le serveur OfficeScan A-2
Configuration requise pour le client OfficeScan A-3
Limitations des serveurs IPv6 purs A-3

Limitations des clients OfficeScan IPv6 purs A-4
Configuration des adresses IPv6 ..... A-6
Écrans affichant les adresses IP A-7

Annexe B: Prise en charge de Windows Server Core 2008

Prise en charge de Windows Server Core 2008 ..... B-2
Méthodes d'installation de Windows Server Core B-2
Installation du client OfficeScan à l'aide de l'outil de Configuration du script de connexion B-3
Installation du client OfficeScan en utilisant à l'aide d'un pack client OfficeScan B-4
Fonctionnalités du client OfficeScan sur Windows Server Core B-6
Commandes Windows Server Core B-7

Annexe C: glossaire

ActiveUpdate C-2
Fichier compressé C-2
Cookie C-2
Refus de service (DoS) C-2
DHCP C-3
DNS C-3
Nom de domaine C-3
Adresse IP dynamique C-4
ESMTP C-4
Contrat de licence utilisateur final C-4
Faux positif C-4
FTP C-5
GeneriClean C-5
Correctif de type hotfix C-5

HTTP C-6
HTTPS C-6
ICMP C-6
IntelliScan C-6
IntelliTrap C-7
IP C-7
Fichier Java C-8
LDAP C-8
Port d'écoute C-8
Agent MCP C-8
Menaces combinées C-9
NAT C-9
NetBIOS C-9
Communication unilatérale C-9
Patch C-10
Attaque de phishing C-10
Ping C-11
POP3 ..... C-11
Serveur proxy C-11
RPC C-11
Correctif de sécurité C-12
Service Pack C-12
SMTP C-12
SNMP C-12
Déroutement SNMP C-12
SOCKS°4 ..... C-13
SSL C-14

Certificat SSL C-14

TCP C-14

Telnet C-14

Port des chevaux de Troie C-14

Port sécurisé C-16
Détermination des ports sécurisés C-16

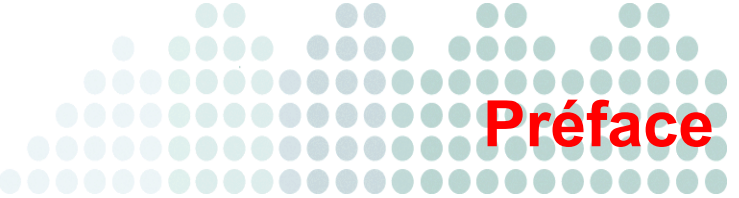
Communication bilatérale C-17

UDP C-17

Fichier non nettoyable C-17
Fichiers infectés par des chevaux de Troie C-17

Index

Index IN-1



Préface

Bienvenue dans le *Manuel de l'administrateur* de Trend Micro™OfficeScan™. Ce document aborde les informations relatives au démarrage, les procédures d'installation client et l'administration du serveur OfficeScan et du client.

Sujets abordés dans ce chapitre:

- *Documentation OfficeScan à la page 2*
- *Public cible à la page 3*
- *Conventions typographiques du document à la page 3*
- *Terminologie à la page 4*

Documentation OfficeScan

La documentation OfficeScan comprend les documents suivants :

TABLEAU 1. Documentation OfficeScan

DOCUMENTATION	DESCRIPTION
Guide d'installation et de mise à niveau	Document PDF qui aborde les éléments requis et les procédures d'installation du serveur OfficeScan, ainsi que les informations nécessaires pour la mise à niveau du serveur et des clients.
Manuel de l'administrateur	document PDF qui aborde les informations relatives au démarrage, les procédures d'installation client et l'administration du serveur OfficeScan et du client
Aide	Fichiers HTML compilés au format WebHelp ou CHM contenant des descriptions de procédures, des conseils d'utilisation et des informations relatives aux champs. L'Aide est accessible depuis les consoles du serveur OfficeScan, du client et du Serveur Policy Server, ainsi que depuis la configuration générale d'OfficeScan.
Fichier Lisez-moi	contient une liste des problèmes connus et les étapes d'installation de base. Il peut aussi contenir des informations relatives au produit qui n'ont pas pu être intégrées à temps dans l'aide ou dans la documentation imprimée
Base de connaissances	Base de données en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les dernières informations sur les problèmes connus identifiés pour les produits. Pour accéder à la base de connaissances, consultez le site Web suivant : http://esupport.trendmicro.com

Téléchargez les versions les plus récentes des documents PDF et du fichier Lisez-moi à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Public cible

La documentation OfficeScan est destinée aux catégories d'utilisateurs suivantes :

- **AdministrateursOfficeScan** : responsables de l'administration d'OfficeScan, ce qui inclut la gestion et l'installation du serveur OfficeScan et du client OfficeScan. Ces utilisateurs sont supposés posséder des connaissances approfondies dans le domaine de la gestion des réseaux et des serveurs.
- **Administrateurs Cisco NAC** : responsables de la conception et de la maintenance des systèmes de sécurité avec les serveurs Cisco NAC et l'équipement réseau Cisco. Ils sont supposés être expérimentés dans l'utilisation de cet équipement.
- **Utilisateurs finaux** : utilisateurs qui ont installé le client OfficeScan sur leur ordinateur. leur niveau de compétence en informatique va du débutant à l'expert.

Conventions typographiques du document

Pour faciliter la recherche et la compréhension des informations, la documentation OfficeScan utilise les conventions suivantes :

TABLEAU 2. Conventions typographiques du document

NOMENCLATURE	DESCRIPTION
MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets, options et tâches
Italique	Références à d'autres documents ou nouveaux composants technologiques
Ordinateurs en réseau > **Paramètres clients généraux**	« Chemin de navigation » indiqué au début des procédures qui aide les utilisateurs à naviguer vers l'écran approprié de la console Web. La présence de plusieurs chemins de navigation indique qu'il existe plusieurs façons d'accéder à un même écran.

NOMENCLATURE	DESCRIPTION
<Texte>	Indique que le texte entre crochets doit être remplacé par les données elles-mêmes. Par exemple, `C:\Program Files\<nom_fichier>` peut correspondre à `C:\Program Files\sample.jpg`.
Remarque	Fournit des recommandations ou des remarques de configuration
Conseil	Informe sur les pratiques recommandées et les recommandations de Trend Micro
AVERTISSEMENT!	Procure des avertissements sur les activités susceptibles de nuire aux ordinateurs de votre réseau

Terminologie

Le tableau ci-dessous présente la terminologie officielle employée dans toute la documentation OfficeScan :

TABLEAU 3. Terminologie OfficeScan

TERMINOLOGIE	DESCRIPTION
Client OfficeScan	Programme client OfficeScan
Ordinateur client	L'ordinateur sur lequel le client OfficeScan est installé
Utilisateur client (ou utilisateur)	Personne qui gère le client OfficeScan sur l'ordinateur client
Serveur	Programme serveur OfficeScan
Ordinateur serveur	L'ordinateur sur lequel le serveur OfficeScan est installé
Administrateur (ou administrateur OfficeScan)	Personne qui gère le serveur OfficeScan

TERMINOLOGIE	DESCRIPTION
Console	L'interface utilisateur permettant de configurer et de gérer les paramètres des serveurs et des clients OfficeScan La console employée pour le programme server OfficeScan est appelée « console Web » et celle employée pour le programme client OfficeScan est appelée « console client ».
Risque liés à la sécurité	Terme générique regroupant les virus/programmes malveillants, les spywares/graywares et les menaces Internet
Service licence	Inclut les services antivirus, Damage Cleanup Services, les services de réputation de sites Web et anti-spyware, qui sont tous activés lors de l'installation du serveur OfficeScan
Service OfficeScan	Services hébergés via Microsoft Management Console (MMC). Par exemple, `ofcservice.exe`, le service principal d'OfficeScan.
Programme	Inclut le client OfficeScan, Cisco Trust Agent et Plug-In Manager
Composants	Responsables du scan, de la détection et des actions contre les risques liés à la sécurité

`Dossier d'installation du client`	Dossier de l'ordinateur qui contient les fichiers du client OfficeScan. Si vous acceptez les paramètres par défaut pendant l'installation, vous trouverez le dossier d'installation à l'un des emplacements suivants :
	
	`C:\Program Files\Trend Micro\OfficeScan Client`
	
	`C:\Program Files\Trend Micro (x86)\OfficeScan Client`

TERMINOLOGIE	DESCRIPTION

`Dossier d'installation du serveur`	Dossier de l'ordinateur qui contient les fichiers du serveur OfficeScan. Si vous acceptez les paramètres par défaut pendant l'installation, vous trouverez le dossier d'installation à l'un des emplacements suivants :
	`C:\Program Files\Trend Micro\OfficeScan`
	`C:\Program Files\Trend Micro (x86)\OfficeScan`
	Par exemple, si un fichier particulier se trouve dans `\PCCSRV` du dossier d'installation du serveur, le chemin d'accès complet au fichier est le suivant :
	`C:\Program Files\Trend Micro\OfficeScan\PCCSRV \<nom_fichier>`.

Client Smart Scan	Client OfficeScan qui a été configuré pour utiliser Smart Scan
Client de scan traditionnel	Client OfficeScan qui a été configuré pour utiliser le scan traditionnel
Double pile	Une entité ayant à la fois une adresse IPv4 et une adresse IPv6. Par exemple : • Un point final à double pile est un ordinateur ayant à la fois une adresse IPv4 et une adresse IPv6. • Un client à double pile est un client installé sur un point final à double pile. • Un agent de mise à jour à double pile propose des mises à jour aux clients. • Un serveur proxy à double pile, tel que DeleGate, peut passer d'une adresse IPv4 à IPv6.
IPv4 pur	Une entité n'ayant qu'une adresse IPv4
IPv6 pur	Une entité n'ayant qu'une adresse IPv6
Solutions de plug-in	Fonctionnalités natives d'OfficeScan et programmes plug-in proposés via Plug-In Manager

Chapitre 1

Présentation d'OfficeScan

Ce chapitre présente Trend Micro™OfficeScan™ et offre un aperçu de ses fonctions et fonctionnalités.

Sujets abordés dans ce chapitre :

- *À propos d'OfficeScan à la page 1-2*
- *Nouveautés de cette version à la page 1-2*
- *Fonctionnalités et avantages principaux à la page 1-9*
- *Le serveur OfficeScan à la page 1-12*
- *Le client OfficeScan à la page 1-13*
- *Intégration aux produits et services de Trend Micro à la page 1-14*

À propos d'OfficeScan

Trend Micro ™OfficeScan™ protège les réseaux d'entreprise contre les programmes malveillants, les virus réseau, les menaces provenant d'Internet, les spywares et les attaques mixtes. Solution intégrée, OfficeScan est composé d'un programme client OfficeScan résidant au point final et d'un programme serveur qui gère tous les clients. Le client OfficeScan protège l'ordinateur et communique au serveur son état de sécurité. Le serveur, via une console d'administration à interface Web, facilite l'application coordonnée de stratégies pour la sécurité et le déploiement des mises à jour vers chaque client.

OfficeScan fonctionne sous Trend Micro Smart Protection Network™, une infrastructure de contenu client en ligne de nouvelle génération qui offre une sécurité plus intelligente que celle des méthodes classiques. La technologie en ligne unique et l'allégement du client réduisent le besoin de téléchargements conventionnels de fichiers de signatures et éliminent les retards couramment associés aux mises à jour des postes de travail. Les entreprises bénéficient d'une augmentation de la bande passante réseau, d'une réduction de la puissance de traitement et d'une diminution des coûts générés. Les utilisateurs accèdent immédiatement à la protection la plus récente où qu'ils se connectent, du réseau de l'entreprise, de leur domicile ou en déplacement.

Nouveautés de cette version

Trend Micro OfficeScan inclut les nouvelles fonctionnalités et améliorations suivantes.

Gestion des stratégies depuis Control Manager

Control Manager 6.0 permet aux administrateurs de créer et de déployer des stratégies sur les serveurs OfficeScan gérés par Control Manager. Pour plus de détails, reportez-vous au Manuel de l'administrateur de Control Manager.

Compatibilité de la surveillance des comportements avec une architecture 64 bits

La fonction de surveillance des comportements d'OfficeScan prend désormais en charge les versions 64 bits des plates-formes suivantes :

- Windows Server 2008™
- Windows 7™
- Windows Vista™ SP1 (ou supérieur)

Compatibilité de l'autoprotection client avec une architecture 64 bits

L'autoprotection client prend désormais en charge les versions 64 bits des plates-formes suivantes :

- Windows Server 2008™
- Windows 7™
- Windows Vista™ SP1 (ou supérieur)

Compatibilité du contrôle des dispositifs avec une architecture 64 bits lors de la prévention des modifications non autorisées

La fonction de contrôle des dispositifs d'OfficeScan prend désormais en charge les versions 64 bits des plates-formes suivantes lors de l'exécution de la prévention des modifications non autorisées :

- Windows 2008™
- Windows 7™
- Windows Vista™ SP1 (ou supérieur)

Remarque

La fonction de protection des données du contrôle des dispositifs est compatible avec toutes les versions 64 bits des plates-formes Windows. Pour des détails sur la configuration des autorisations 64 bits, voir *Autorisations pour les périphériques de stockage à la page 8-3*.

Améliorations apportées à la protection des données

Les améliorations apportées à la protection des données dans OfficeScan 10.6 SP1 comprennent la prise en charge et les mises à niveau suivantes :

- La prise en charge des versions 64 bits des plates-formes Windows par la fonction de Prévention contre la perte de données et le contrôle des dispositifs
- Plus de 100 nouveaux modèles de Prévention contre la perte de données préconfigurés et des identificateurs de données.

Améliorations de Virtual Desktop Infrastructure

Cette version d'OfficeScan améliore la compatibilité et les capacités de Virtual Desktop Infrastructure (VDI).

- **Prise en charge de Microsoft Hyper-V™** : Les administrateurs peuvent également gérer les clients virtuels avec le serveur Microsoft Hyper-V™ en plus des serveurs VMware vCenter™ et Citrix XenServer™.
- **Amélioration des environnements non persistants** : OfficeScan identifie désormais les clients virtuels par leur adresse Media Access Control (MAC). Ceci empêche OfficeScan d'attribuer plusieurs identificateurs globaux uniques (GUID) au même client dans les environnements non persistants.

Pour obtenir des informations détaillées, voir *Trend Micro Virtual Desktop Support à la page 13-76*.

Scan étendu des ports dans le cadre des stratégies de réputation des sites Web

OfficeScan peut à présent scanner le trafic HTTP sur l'ensemble des ports à la recherche de violations de la stratégie de réputation de sites Web. Si les administrateurs ne

souhaitent pas scanner le trafic sur tous les ports, OfficeScan permet de ne scanner le trafic que sur les ports HTTP 80, 81 et 8080 par défaut.

Pour obtenir des informations détaillées, voir *Configuration de Stratégie de réputation de sites Web à la page 10-3*.

Nouveautés de la version 10.6

Trend Micro OfficeScan 10.6 inclut les nouvelles fonctionnalités et améliorations suivantes.

- **Protection des données**

  Le module Protection des données fournit une Prévention contre la perte de données et élargit l'éventail des dispositifs surveillés par le contrôle des dispositifs.

  Plug-In Manager gère l'installation et les licences du module de Protection des données. Pour plus d'informations, voir *Installation de la protection des données à la page 9-2*.

  TABLEAU 1-1. Fonctionnalités de la protection des données OfficeScan

FONCTIONS DE PROTECTION DES DONNÉES	DÉTAILS
Prévention contre la perte de données	La prévention contre la perte de données protège les actifs numériques d'une entreprise contre les fuites de données, délibérées ou accidentelles. La prévention contre la perte des données permet ce qui suit : • L'identification de l'actif numérique à protéger • La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes. • Le renforcement de la conformité à des normes de confidentialité établies Pour plus d'informations, voir *À propos de la prévention contre la perte de données à la page 9-9*.

FONCTIONS DE PROTECTION DES DONNÉES	DÉTAILS
Contrôle des dispositifs	OfficeScan intègre par défaut une fonction Contrôle des dispositifs qui régule l'accès aux périphériques de stockage USB, CD/DVD, disquettes et lecteurs réseau. Le contrôle des dispositifs, qui fait partie du module de protection des données, élargit l'éventail des dispositifs en régulant l'accès aux périphériques suivants : • Périphériques d'images • Modems • Ports (COM et LPT) • Périphériques infrarouges • Cartes PCMCIA • Touche Impr. écran • Interface IEEE 1394 Pour plus d'informations, voir *Contrôle des dispositifs à la page 8-2*.

- **Plug-in Manager 2.0**

  Plug-in Manager 2.0 s'installe avec le serveur OfficeScan. Cette version de Plug-in Manager fournit des widgets.

  Les widgets fournissent une référence synthétique des fonctions d'OfficeScan et des plug-in que vous considérez comme essentiels à votre entreprise. Les widgets sont disponibles dans le résumé du tableau de bord d'OfficeScan qui remplace l'écran Résumé des versions précédentes d'OfficeScan. Pour plus d'informations, voir *Le tableau de bord récapitulatif à la page 2-5*.

- **Prise en charge d'IPv6**

  Le serveur et les clients OfficeScan peuvent désormais être installés sur des ordinateurs IPv6.

De plus, les nouvelles versions de Control Manager et de Smart Protection Server prennent désormais en charge l'adressage IPv6 pour fournir une intégration transparente avec le serveur et les clients OfficeScan.

Pour plus d'informations, voir *Prise en charge de l'adressage IPv6 pour les serveurs et les clients OfficeScan. à la page A-2*.

- **Fichiers de mémoire cache pour les scans**

  Le client OfficeScan génère maintenant des fichiers de mémoire cache, qui contiennent des informations sur les fichiers légitimes qui ont été précédemment scannés et les fichiers que Trend Micro considère comme dignes de confiance. Les fichiers de mémoire cache fournissent une référence rapide lors des scans à la demande et diminuent ainsi l'utilisation des ressources système. Les scans à la demande (scan manuel, scan programmé et scan immédiat) sont désormais plus efficaces, avec une rapidité améliorée de 40 %.

  Pour plus d'informations, voir *Paramètres du cache pour les scans à la page 6-65*.

- **Optimisation du démarrage**

  Au démarrage d'un ordinateur, le client OfficeScan diffère le téléchargement de certains services client si l'utilisation de l'UC dépasse les 20 %. Lorsque l'utilisation de l'UC redescend sous cette limite, le client démarre le téléchargement des services.

  Les services comprennent :

  - Pare-feu d'OfficeScan NT
  - Service de protection des données OfficeScan
  - Service de prévention des modifications non autorisées

- **Amélioration apportée à Damage Cleanup Services**

  Damage Cleanup Services peut maintenant fonctionner en mode de nettoyage avancé pour un arrêt des activités par le logiciel de sécurité serveur, également appelé FakeAV. Le client utilise aussi les règles de nettoyage avancé afin de détecter et d'arrêter proactivement les applications qui présentent un comportement FakeAV.

  Vous pouvez choisir le mode de nettoyage lorsque vous configurez des actions de scan antivirus/programmes malveillants pour le scan manuel, le scan en temps réel,

le scan programmé et le scan immédiat. Pour plus d'informations, voir *Damage Cleanup Services à la page 6-42*.

- **Prise en charge du protocole HTTPS par la réputation de sites Web**

  Le client OfficeScan peut désormais être installé sur Windows Server Core 2008. Les utilisateurs peuvent utiliser l'interface de ligne de commande pour lancer la console client et vérifier l'état de la protection du point final.

- **Prise en charge de Windows Server Core 2008**

  Le client OfficeScan peut désormais être installé sur Windows Server Core 2008. Les utilisateurs peuvent utiliser l'interface de ligne de commande pour lancer la console client et vérifier l'état de la protection du point final.

  Pour plus d'informations, voir *Prise en charge de Windows Server Core 2008 à la page B-2*.

- **Autres améliorations**

  Cette version inclut les améliorations suivantes :

  - Les clients Smart Scan exécutent maintenant le scan de la messagerie Outlook en mode Smart Scan. Dans les versions précédentes, les clients Smart Scan exécutaient le scan de la messagerie Outlook en mode de scan traditionnel.
  - Les journaux et les notifications de détection de spywares/graywares affichent désormais le nom de l'utilisateur connecté à l'ordinateur au moment de la détection.
  - Dans les journaux de spywares/graywares, si le résultat du scan de deuxième niveau est «Ignoré», le résultat de scan de premier niveau est désormais «Action supplémentaire requise» au lieu de «Aucune action requise». Grâce à cette amélioration, vous pouvez désormais prendre des mesures supplémentaires telles que le nettoyage des spywares/graywares que vous considérez comme dangereux.
  - L'autoprotection client est désormais un paramètre détaillé que vous pouvez configurer dans l'arborescence des clients.
  - Vous pouvez désormais configurer tous les clients pour qu'ils envoient des messages de battement de cœur au serveur OfficeScan. Dans la version

précédente, seuls les clients de réseaux inaccessibles envoient des messages de battement de cœur. Pour plus d'informations, voir *Clients inaccessibles à la page 13-45*.

- Lors de l'exportation des paramètres de l'arborescence des clients dans un fichier .dat, tous les paramètres sont désormais exportés, à l'exception des paramètres de l'agent de mise à jour. Dans les versions précédentes, seuls les paramètres de scan et les privilèges et autres paramètres du client sont exportés. Pour plus d'informations sur l'exportation des paramètres, consultez la rubrique *Importation et exportation des paramètres du client à la page 13-55*.

- Lorsque vous utilisez l'outil Client Mover, vous pouvez désormais spécifier le sous-domaine de l'arborescence des clients auquel rattacher le client après son déplacement vers son nouveau serveur parent. Pour plus d'informations, voir *Client Mover à la page 13-23*.

Fonctionnalités et avantages principaux

OfficeScan fournit les fonctionnalités et avantages suivants :

- **Plug-In Manager et solutions de plug-in**

  Plug-In Manager facilite l'installation, le déploiement et la gestion des solutions de plug-in.

  Les administrateurs peuvent installer deux types de solutions de plug-in :

  - Programmes plug-in
  - Fonctions natives d'OfficeScan

- **Gestion centralisée**

  Une console d'administration à interface Web offre aux administrateurs un accès transparent à tous les clients et serveurs du réseau. La console Web coordonne le déploiement automatique des stratégies de sécurité, des fichiers de signatures et des mises à jour logicielles sur chaque client et chaque serveur. De plus, grâce à Outbreak Prevention Services, les vecteurs d'infection sont bloqués et les stratégies de sécurité spécifiques aux attaques sont rapidement déployées pour prévenir ou contenir les épidémies avant que les fichiers de signatures ne soient disponibles.

OfficeScan effectue également une surveillance en temps réel, avec notification d'événements et génération de rapports complets. Les administrateurs peuvent procéder à l'administration à distance, définir des stratégies personnalisées pour des postes de travail ou groupes individuels et verrouiller les paramètres de sécurité du client.

- **Protection contre les risques de sécurité**

  OfficeScan protège les ordinateurs contre les risques de sécurité en scannant les fichiers avant de mener une action spécifique selon chaque risque détecté. Un nombre élevé de risques de sécurité détectés en peu de temps témoigne d'une épidémie. Pour enrayer les épidémies, OfficeScan applique des stratégies de prévention des épidémies et isole les ordinateurs sur lesquels sont détectés les fichiers infectés jusqu'à ce qu'ils ne présentent plus aucun risque.

  OfficeScan utilise Smart Scan pour optimiser l'efficacité du processus de scan. Cette technologie consiste à transférer un nombre important de signatures précédemment stockées sur l'ordinateur local vers un serveur Sources Smart Protection. Cette démarche réduit considérablement l'impact sur les systèmes et sur le réseau du volume sans cesse croissant de mises à jour de signatures vers les points finaux.

  Pour plus d'informations concernant Smart Scan et son déploiement sur les clients, voir *Méthodes de scan à la page 6-8*.

- **Damage Cleanup Services**

  Damage Cleanup Services™ débarrasse les ordinateurs des virus basés sur fichiers et des virus de réseau, ainsi que des résidus de virus et de vers (chevaux de Troie, entrées de registre, fichiers viraux) et ce, à l'aide d'un processus totalement automatisé. Pour traiter les menaces et les nuisances générées par les chevaux de Troie, Damage Cleanup Services effectue les actions suivantes :

  - Détecte et supprime les chevaux de Troie actifs
  - Élimine les processus créés par les chevaux de Troie
  - Répare les fichiers système modifiés par les chevaux de Troie
  - Supprime les fichiers et les applications laissés par les chevaux de Troie

  Les services Damage Cleanup Services s'exécutent automatiquement en arrière-plan ; vous n'avez donc pas besoin de les configurer. Les utilisateurs ne remarquent

même pas son activité. Toutefois, OfficeScan peut parfois demander à l'utilisateur de redémarrer son ordinateur pour terminer la procédure de suppression des chevaux de Troie.

- **Réputation de sites Web**

  La technologie de réputation de sites Web protège proactivement les ordinateurs clients au sein ou en-dehors du réseau d'entreprise contre les sites Web malveillants et potentiellement dangereux. La réputation de sites Web rompt la chaîne d'infection et empêche le téléchargement de code malveillant.

  Vérifiez la crédibilité des sites et des pages Web en intégrant OfficeScan au serveur Smart Protection Server ou à Trend Micro Smart Protection Network.

- **Pare-feu OfficeScan**

  Le pare-feu OfficeScan protège les clients et les serveurs du réseau grâce à une fonction Stateful inspection et à des scans antivirus de réseau haute performance. Créez des règles pour filtrer les connexions par application, adresse IP, numéro de port ou protocole, puis appliquez-les à différents groupes d'utilisateurs.

- **Prévention contre la perte de données**

  La prévention contre la perte de données protège les actifs numériques d'une entreprise contre les fuites de données, délibérées ou accidentelles. La prévention contre la perte des données permet aux administrateurs ce qui suit :

  - L'identification de l'actif numérique à protéger
  - La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes.
  - Le renforcement de la conformité à des normes de confidentialité établies

- **Contrôle des dispositifs**

  Le Contrôle des dispositifs régule l'accès aux périphériques de stockage externes et ressources réseau connectés aux ordinateurs. Le Contrôle des dispositifs prévient la perte et les fuites de données et, conjointement avec le scan de fichiers, contribue à la protection contre les risques de sécurité.

- **Surveillance des comportements**

La surveillance des comportements surveille continuellement les clients, guettant les modifications inhabituelles du système d'exploitation ou des logiciels installés.

- **Application de la sécurité et des stratégies**

  OfficeScan permet une intégration transparente de Cisco™ Trust Agent, qui fournit l'application des stratégies la plus efficace au sein d'un réseau à autodéfense de Cisco (Cisco Self-Defending Network). Il inclut également un serveur Policy Server pour une communication automatique avec des serveurs Cisco Access Control Server. Une fois intégré à Trend Micro™ Network VirusWall™ ou à tout dispositif Network Admission Control (NAC), OfficeScan peut contrôler les clients tentant d'accéder au réseau puis corriger, rediriger, restreindre, refuser ou autoriser l'accès. Si un ordinateur est vulnérable ou est infecté, OfficeScan peut automatiquement l'isoler de même que les segments du réseau correspondants jusqu'à ce que tous les ordinateurs soient à jour ou jusqu'à ce que le nettoyage soit terminé.

Le serveur OfficeScan

Le serveur OfficeScan est un référentiel central contenant l'ensemble des configurations des clients, des journaux de risques de sécurité et des mises à jour.

Le serveur exécute deux tâches primordiales :

- il installe, surveille et gère les clients OfficeScan,
- Il télécharge la plupart des composants dont les clients ont besoin. Le serveur OfficeScan télécharge les composants depuis le serveur Trend Micro ActiveUpdate puis les distribue aux clients.

Remarque

Certains composants sont téléchargés par les sources Smart Protection. Voir *Sources Smart Protection à la page 3-6* pour obtenir des informations détaillées.

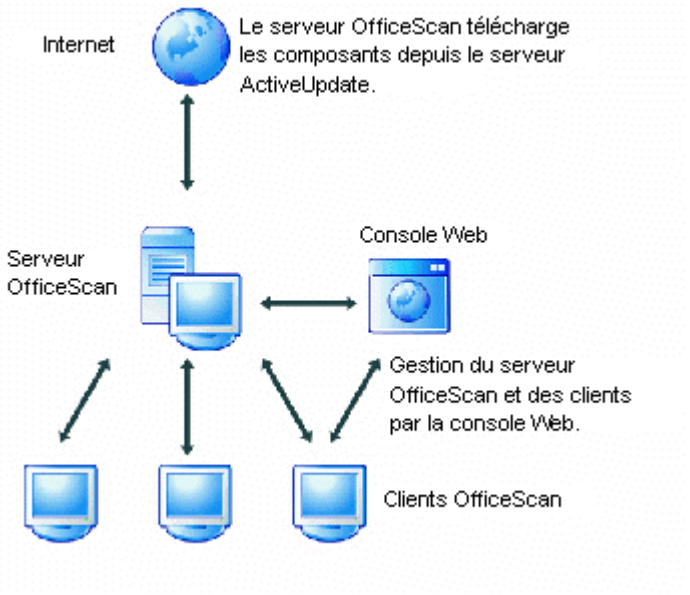

Internet
Le serveur OfficeScan télécharge les composants depuis le serveur ActiveUpdate.
Serveur OfficeScan
Console Web
Gestion du serveur OfficeScan et des clients par la console Web.
Clients OfficeScan

FIGURE 1-1. Fonctionnement du serveur OfficeScan

Le serveur OfficeScan est capable d'établir une communication bidirectionnelle en temps réel entre le serveur et les clients. Gérez les clients depuis une console Web basée sur un navigateur à laquelle les administrateurs peuvent accéder depuis la quasi-totalité du réseau. Le serveur communique avec le client (et le client avec le serveur) via le protocole HyperText Transfer Protocol (HTTP).

Le client OfficeScan

Vous pouvez protéger les ordinateurs Windows contre les risques relatifs à la sécurité en installant le client OfficeScan sur chaque ordinateur.

Le client OfficeScan dépend du serveur parent à partir duquel il a été installé. Vous pouvez configurer les clients pour qu'ils dépendent d'autres serveurs en utilisant l'outil Client Mover. Le client envoie serveur en temps réel les informations relatives à l'état et

aux événements. Les événements transmis sont notamment la détection d'un virus/programme malveillant, le démarrage d'un client, la déconnexion d'un client, le lancement d'un scan et la réalisation d'une mise à jour.

Intégration aux produits et services de Trend Micro

OfficeScan s'intègre aux produits et services Trend Micro mentionnés dans le tableau suivant. Pour une intégration sans difficulté, assurez-vous que les produits fonctionnent avec les versions requises ou recommandées.

TABLEAU 1-2. Produits et services qui s'intègrent à OfficeScan

PRODUIT/ SERVICE	DESCRIPTION	VERSION
Serveur ActiveUpdate	Fournit tous les composants nécessaires au client d'OfficeScan pour protéger les clients des menaces de sécurité	Sans objet
Smart Protection Network	Fournit aux clients des services de File Reputation et des services de réputation de sites Web. Smart Protection Network est hébergé par Trend Micro.	Sans objet

PRODUIT/ SERVICE	DESCRIPTION	VERSION
Serveur Smart Protection Server autonome	Fournit les mêmes services de File Reputation et de réputation de sites Web que Smart Protection Network. Un serveur autonome Smart Protection Server est destiné à localiser le service sur le réseau de l'entreprise afin d'assurer une efficacité optimale. **Remarque** Un serveur Smart Protection Server intégré est installé sur le serveur OfficeScan Server. Il possède les mêmes fonctions que le serveur autonome, mais ses capacités sont limitées.	• 2.5 (recommandé) • 2.0
Control Manager	Solution de gestion logicielle vous permettant de contrôler l'antivirus et les programmes de sécurisation du contenu depuis un emplacement central, indépendamment de la plate-forme ou de l'emplacement physique du programme.	• 6.0 (recommandé) • 5.5 SP1 • 5.5 • 5.0

Chapitre 2

Démarrage d'OfficeScan

Ce chapitre décrit comment démarrer avec Trend Micro™OfficeScan™ et les paramètres de configuration initiaux.

Sujets abordés dans ce chapitre :

- *La console Web à la page 2-2*
- *Le tableau de bord récapitulatif à la page 2-5*
- *Intégration d'Active Directory à la page 2-27*
- *L'arborescence des clients OfficeScan à la page 2-31*
- *Domaines OfficeScan à la page 2-44*

La console Web

La console Web est le point central permettant de surveiller sur l'ensemble du réseau de l'entreprise. La console présente des paramètres et des valeurs par défaut que vous pouvez configurer en fonction de vos spécifications et exigences de sécurité. La console Web utilise des technologies Internet standard telles que Java, CGI, HTML et HTTP.

Remarque

Configurez les paramètres de délai d'attente depuis la console Web. Voir la section *Paramètres de la console Web à la page 12-46*.

Utilisez la console Web pour effectuer les opérations suivantes :

- Gérer les clients installés sur les ordinateurs en réseau
- Regrouper les clients par domaines logiques pour permettre de les configurer et de les gérer tous ensemble
- Définir des configurations de scan et lancer un scan manuel sur un ou plusieurs ordinateurs en réseau
- Configurer les notifications sur les risques liés à la sécurité affectant le réseau et afficher les journaux envoyés par les clients
- Configurer les critères et les notifications d'épidémie
- Déléguer des tâches d'administration de la console Web à d'autres administrateurs OfficeScan en configurant les rôles et les comptes utilisateurs
- S'assurer que les clients respectent les consignes de sécurité

Configuration requise pour l'ouverture de la console Web

Ouvrez la console Web depuis tout ordinateur du réseau disposant des ressources suivantes :

- Processeur Intel™ Pentium™ 300MHz ou équivalent
- 128 Mo de mémoire vive

- Au moins 30 Mo d'espace disque disponible
- Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum
- Microsoft Internet Explorer™ 7.0 ou version supérieure

Sur le navigateur Web, entrez l'une des adresses suivantes dans la barre d'adresses en fonction du type d'installation du serveur OfficeScan :

TABLEAU 2-1. URL de la console Web d'OfficeScan

TYPE D'INSTALLATION	URL
Sans SSL sur un site par défaut	`http://<Nom de domaine complet ou adresse IP du serveur OfficeScan>/OfficeScan`
Sans SSL sur un site virtuel	`http://<Nom de domaine complet ou adresse IP du serveur OfficeScan>:<Numéro de port HTTP>/OfficeScan`
Avec SSL sur un site par défaut	`https://<Nom de domaine complet ou adresse IP du serveur OfficeScan>/OfficeScan`
Avec SSL sur un site virtuel	`https://<Nom de domaine complet ou adresse IP du serveur OfficeScan>/OfficeScan`

Remarque

Si vous avez procédé à une mise à niveau à partir d'une version antérieure OfficeScan, les fichiers de mémoire cache du serveur proxy et du navigateur Web peuvent empêcher le chargement correct de la console Web d'OfficeScan. Videz la mémoire cache du navigateur et celle de tout serveur proxy situé entre le serveur OfficeScan et l'ordinateur que vous utilisez pour accéder à la console Web.

Compte de connexion

Pendant l'installation du serveur OfficeScan, le programme d'installation crée un compte racine et vous invite à saisir le mot de passe de ce compte. Lors de la première ouverture

de la console Web, saisissez «racine» comme nom d'utilisateur et mot de passe de compte racine. Si vous avez oublié votre mot de passe, contactez votre service d'assistance pour qu'il vous aide à le réinitialiser.

Définissez des rôles utilisateurs et configurez les comptes utilisateurs de façon à permettre à d'autres utilisateurs d'accéder à la console Web sans employer le compte racine. Lorsqu'ils se connectent, les utilisateurs peuvent se servir des comptes utilisateurs que vous avez configurés pour eux. Pour plus d'informations, voir *Administration basée sur les rôles à la page 12-2*.

La bannière de la console Web

Dans la zone bannière de la console Web, vous disposez des options suivantes :

FIGURE 2-1. Zone bannière de la console Web

- **<nom de compte>** : cliquez sur le nom du compte (par exemple, racine) pour changer des informations du compte (par exemple, le mot de passe).
- **Déconnexion** : vous déconnecte de la console Web
- **Aide** ( )
  - **Nouveautés** : ouvre une page contenant une liste de nouvelles fonctionnalités incluses dans la version actuelle du produit
  - **Sommaire et index** : ouvre l'aide du serveur OfficeScan
  - **Base de connaissances** : permet d'ouvrir la base de connaissances de Trend Micro depuis laquelle vous pouvez accéder aux questions fréquemment posées (FAQ), à des informations actuelles sur les produits Trend Micro et au service d'assistance client, ainsi qu'enregistrer OfficeScan
  - **Infos Sécurité** : affiche la page d'informations de sécurité Trend Micro ; vous y trouverez des informations sur les derniers risques de sécurité

- **Service commercial**: affiche la page Web du service commercial de Trend Micro sur laquelle vous pouvez contacter votre distributeur local
- **Assistance** : affiche la page Web d'assistance technique de Trend Micro, sur laquelle vous pouvez poser des questions et trouver des réponses aux questions les plus fréquentes concernant les produits Trend Micro
- **À propos de**: fournit une vue d'ensemble du produit, des instructions pour vérifier les détails des versions de composants et un lien vers Assistance Intelligence System. Pour obtenir des informations détaillées, voir *Support Intelligence System à la page 17-2*.

Le tableau de bord récapitulatif

Le tableau de bord **Résumé** s'affiche lorsque vous ouvrez la console Web OfficeScan ou cliquez sur **Résumé** dans le menu principal.

Chaque compte utilisateur de la console Web dispose d'un tableau de bord totalement indépendant. Aucun changement dans les paramètres de tableau de bord d'un compte utilisateur n'affectera les tableaux de bord des autres comptes utilisateurs.

Si un tableau de bord contient les données d'un client OfficeScan, les données s'affichant dépendent des autorisations sur le domaine client pour le compte utilisateur. Par exemple, si vous accordez à un compte utilisateur les autorisations de gérer les domaine A et B, le tableau de bord du compte utilisateur n'affichera que les données des clients appartenant aux domaines A et B.

Pour obtenir des détails sur les comptes utilisateurs, voir *Administration basée sur les rôles à la page 12-2*.

Le tableau de bord **Résumé** comprend les éléments suivants :

- Section de l'état de la licence de produit
- Widgets
- Onglets

Section de l'état de la licence de produit

Cette section se situe au-dessus du tableau de bord et affiche l'état des licences OfficeScan.

Résumé
Actualiser
Aide
De nouveaux widgets peuvent être mis à jour.
Mettre à jour
Services activés: Antivirus pour serveur/poste de travail, Réputation de sites Web de postes de travail/serveurs et anti-spyware, File Reputation, Pare-feu , Damage Cleanup Services

FIGURE 2-2. Section de l'état de la licence de produit

Des messages de rappel concernant l'état de la licence s'affichent dans les cas suivants :

- Si vous possédez une licence de version complète :
  - 60 jours avant l'expiration d'une licence
  - Pendant la période de grâce du produit. La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro.
  - Une fois la licence expirée et la période de grâce écoulée: pendant cette période, vous ne pourrez ni obtenir d'assistance technique ni effectuer de mises à jour des composants. Les moteurs de scan continueront à scanner les ordinateurs à l'aide des composants obsolètes. Ces composants obsolètes ne peuvent pas vous protéger entièrement contre les derniers risques de sécurité.
- Si vous disposez d'une licence pour la version d'évaluation :
  - 14 jours avant l'expiration d'une licence
  - Une fois la licence expirée: Pendant cette période, OfficeScan désactive les mises à jour et le scan des composants, ainsi que toutes les fonctionnalités des clients.

Si vous avez obtenu un code d'activation, renouvelez votre licence en accédant à **Administration** > **Licence du produit**.

Onglets et widgets

Les widgets constituent les composants centraux du tableau de bord. Les widgets fournissent des informations spécifiques sur les différents événements liés à la sécurité. Certains widgets vous permettent d'exécuter certaines tâches, telles que la mise à jour de vieux composants.

Les informations fournies par un widget proviennent des sources suivantes :

- Le serveur et les clients OfficeScan
- Les solutions de plug-in et leurs agents côté client
- Trend Micro Smart Protection Network

Remarque

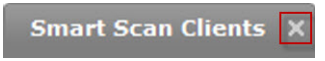
Activez Smart Feedback afin d'afficher les données de Smart Protection Network. Pour plus d'informations sur Smart Feedback, voir *Smart Feedback à la page 12-51*.

Les onglets fournissent un endroit pour accueillir les widgets. Le tableau de bord récapitulatif peut accueillir jusqu'à 30 onglets.

Utilisation des onglets

Gérez les onglets en exécutant les tâches suivantes :

TABLEAU 2-2. Tâches via les onglets

TÂCHE	ÉTAPES
Ajouter un nouvel onglet	1. Cliquez sur l'icône Ajouter situé au-dessus du tableau de bord. Un nouvel écran s'affiche. 2. Indiquez ce qui suit : • **Titre** : le nom de l'onglet • **Disposition** : choisissez parmi les dispositions disponibles • **Ajustement automatique** : pour sélectionner une disposition contenant plusieurs zones (telle que « »), chaque zone ne contenant qu'un seul widget. L'ajustement automatique ajuste un a widget afin qu'il rentre dans la zone. 3. Cliquez sur **Enregistrer**.
Modifier les paramètres d'onglets	1. Cliquez sur **Paramètres d'onglets** dans l'angle droit de l'onglet. Un nouvel écran s'affiche. 2. Modifiez le nom de l'onglet, sa disposition et ses paramètres d'ajustement automatique. 3. Cliquez sur **Enregistrer**.
Déplacer un onglet	Utilisez le glisser-déplacer pour déplacer un onglet.
Supprimer un onglet	Cliquez sur l'icône Supprimer située à côté du titre de l'onglet.  La suppression d'un onglet supprime également tous les widgets de l'onglet.

Utilisation des widgets

Gérez les widgets en exécutant les tâches suivantes :

TABLEAU 2-3. Tâches des widgets

TÂCHE	ÉTAPES
Ajouter un nouveau widget	1. Cliquez sur un onglet. 2. Cliquez sur **Ajouter des widgets** dans l'angle supérieur droit de l'onglet. Un nouvel écran s'affiche. 3. Sélectionnez les widgets à ajouter. Pour une liste des widgets disponibles, voir *Widgets disponibles à la page 2-11*. • Cliquez sur les icônes d'affichage ( ) en haut à droite de l'écran afin de basculer entre l'affichage Détaillé et l'affichage Résumé. • À gauche de l'écran se trouvent les catégories de widgets. Sélectionnez une catégorie afin d'affiner les sélections. • Utilisez la zone de recherche de texte située en haut de l'écran afin de rechercher un widget spécifique. 4. Cliquez sur **Ajouter**.
Déplacer un widget	Utilisez le glisser-déplacer pour déplacer un widget dans une zone différente à l'intérieur de l'onglet.
Redimensionner un widget	Redimensionnez un widget dans un onglet à plusieurs colonnes en pointant le curseur sur l'angle droit du widget, puis en déplaçant le curseur vers la gauche ou la droite.
Modifier le titre du widget	1. Cliquez sur l'icône Modifier ( ). Un nouvel écran s'affiche. 2. Saisissez le nouveau titre. **Remarque** Pour certains widgets, tels que le Mashup d'OfficeScan et des plug-ins, des éléments liés aux widgets peuvent être modifiés. 3. Cliquez sur **Enregistrer**.

TÂCHE	ÉTAPES
Rafraîchir les données du widget	Cliquez sur l'icône Actualiser ( ).
Supprimer un widget	Cliquez sur l'icône Supprimer ( ).

Onglets et widgets prédéfinis

Le tableau de bord **Résumé** est fourni avec un ensemble d'onglets et de widgets prédéfinis. Vous pouvez renommer ou supprimer ces onglets et widgets.

TABLEAU 2-4. Onglets par défaut dans le tableau de bord Résumé

ONGLET	DESCRIPTION	WIDGETS
OfficeScan	Cet onglet contient les mêmes informations présentes sur l'écran **Résumé** des versions précédentes d'OfficeScan. Dans cet onglet, vous pouvez avoir un aperçu de la protection contre les risques liés à la sécurité du réseau OfficeScan. Vous pouvez également agir sur les éléments nécessitant une intervention immédiate, tels que les épidémies ou les composants obsolètes.	• *Widget Connectivité du client à la page 2-13* • *Widget de détection des risques liés à la sécurité à la page 2-16* • *Widget Épidémies à la page 2-17* • *Widget Mises à jour du client à la page 2-19*
OfficeScan et les plug-ins	Cet onglet présente les clients qui sont exécutés par le client OfficeScan et les solutions de plug-in. Utilisez cet onglet pour évaluer l'état de sécurité général des clients.	*Widget Mashup d'OfficeScan et des plugiciels à la page 2-20*

ONGLET	DESCRIPTION	WIDGETS
Smart Protection Network	Cet onglet contient des informations provenant de Trend Micro Smart Protection Network, qui fournit des services de réputation des fichiers et des sites Web aux clients OfficeScan.	• *Widget Sources majeures des menaces selon la réputation des sites Web à la page 2-24* • *Widget Utilisateurs les plus menacés selon la réputation des sites Web à la page 2-25* • *Widget Carte des menaces de File Reputation à la page 2-26*

Widgets disponibles

Les widgets suivants sont disponibles dans cette version :

TABLEAU 2-5. Widgets disponibles

NOM DU WIDGET	DISPONIBILITÉ
Connectivité du client	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Connectivité du client à la page 2-13*.
Détection des risques liés à la sécurité	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget de détection des risques liés à la sécurité à la page 2-16*.
Épidémies	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Épidémies à la page 2-17*.
Mises à jour du client	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Mises à jour du client à la page 2-19*.

NOM DU WIDGET	DISPONIBILITÉ
Mashup d'OfficeScan et des plugiciels	Disponible et prêt à l'emploi mais n'affiche que les données des clients OfficeScan Les données des solutions de plug-in suivantes sont disponibles après avoir activé chaque solution : • Intrusion Defense Firewall • Trend Micro Virtual Desktop Support Pour obtenir des informations détaillées, voir *Widget Mashup d'OfficeScan et des plugiciels à la page 2-20*.
Incidents majeurs de prévention contre la perte de données	Disponible après avoir activé la protection des données OfficeScan Pour obtenir des informations détaillées, voir *Widget Incidents majeurs de prévention contre la perte de données à la page 2-22*.
Incidents de prévention contre la perte de données dans le temps	Disponible après avoir activé la protection des données OfficeScan Pour obtenir des informations détaillées, voir *Widget Incidents de prévention contre la perte de données dans le temps à la page 2-23*.
Sources majeures des menaces selon la réputation des sites Web	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Sources majeures des menaces selon la réputation des sites Web à la page 2-24*.
Utilisateurs les plus menacés selon la réputation des sites Web	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Utilisateurs les plus menacés selon la réputation des sites Web à la page 2-25*.
Carte des menaces de File Reputation	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Carte des menaces de File Reputation à la page 2-26*.

NOM DU WIDGET	DISPONIBILITÉ
IDF - État d'alerte	Disponible après avoir activé Intrusion Defense Firewall. Pour plus d'informations concernant ces widgets, voir la documentation IDF.
IDF - État de l'ordinateur	
IDF - Historique des événements du réseau	
IDF - Historique des événements du système	

Widget Connectivité du client

Le widget **Connectivité du client** affiche l'état de la connexion des clients antivirus ayant un serveur OfficeScan. Les données s'affichent dans un tableau et un graphique circulaire. Vous pouvez basculer entre le tableau et le graphique circulaire en cliquant sur les icônes d'affichage ( ).

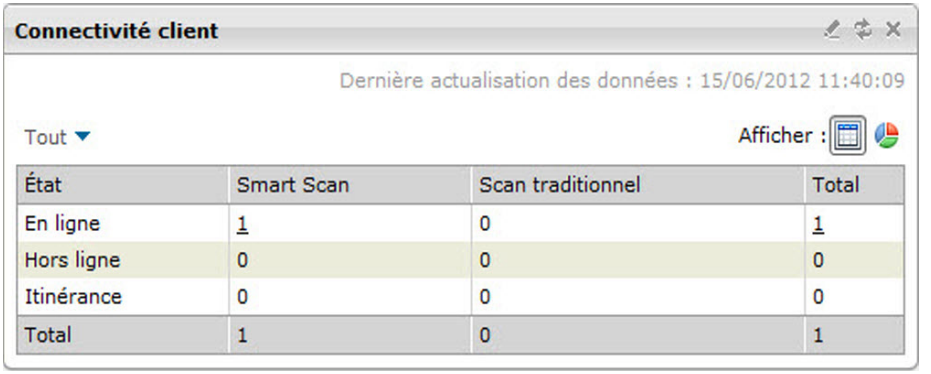


FIGURE 2-3. Widget Connectivité du client affichant un tableau

Widget Connectivité du client sous forme de tableau

Le tableau distingue les clients par méthodes de scan.

Si le nombre de clients pour un état particulier est égal ou supérieur à 1, vous pouvez cliquer sur le nombre afin d'afficher les clients dans l'arborescence des clients. Vous pouvez exécuter des tâches pour ces clients ou modifier leurs paramètres.

Pour afficher uniquement les clients utilisant une méthode de scan particulière, cliquez sur **Tous**, puis sélectionnez la méthode de scan.

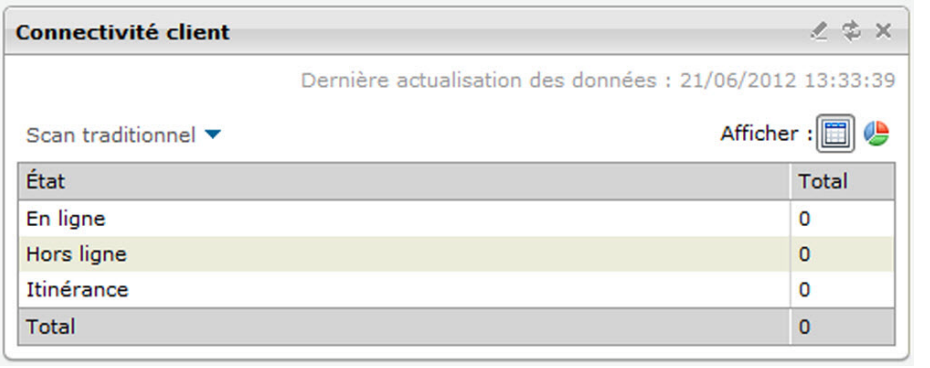


FIGURE 2-4. État de connexion des clients de scan traditionnel

FIGURE 2-5. État de connexion des clients Smart Scan

Si vous avez sélectionné **Smart Scan** :

- Le tableau distingue les clients Smart Scan en ligne en fonction de l'état de connexion avec les serveurs Smart Protection Server.

Remarque

Seuls les clients en ligne peuvent signaler leur état de connexion avec les serveurs Smart Protection Server.

Si des clients sont déconnectés d'un serveur Smart Protection Server, restaurez la connexion en suivant les étapes indiquées à la rubrique *Les sources Smart Protection ne sont pas disponibles à la page 13-42*.

- Chaque serveur Smart Protection Server possède une URL sur laquelle cliquer pour lancer la console du serveur.
- S'il y a plusieurs serveurs Smart Protection Server, cliquez sur **PLUS**. Un nouvel écran s'ouvre, affichant tous les serveurs Smart Protection Server.

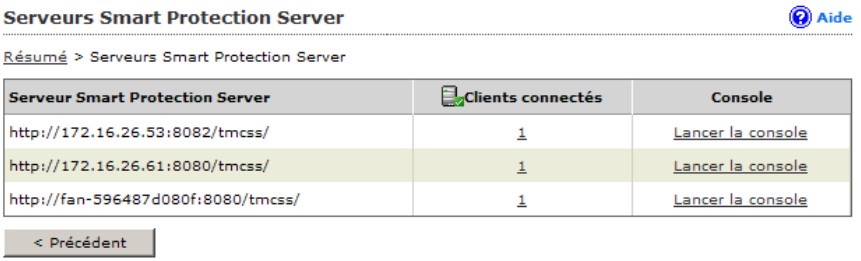


FIGURE 2-6. Liste Serveurs Smart Protection Server

Dans cet écran, vous pouvez :

- Afficher tous les serveurs Smart Protection Server auxquels les clients sont connectés, ainsi que le nombre de clients connectés à chaque serveur. Un clic sur le numéro permet d'ouvrir l'arborescence client depuis laquelle vous pouvez gérer les paramètres clients.
- Lancer une console de serveur en cliquant sur le lien menant au serveur

Widget Connectivité du client sous forme de graphique circulaire

Le graphique circulaire affiche uniquement le nombre de clients pour chaque état et ne distingue pas les clients en fonction des méthodes de scan. Cliquer sur un statut permet de le séparer ou de le reconnecter au reste du graphique.

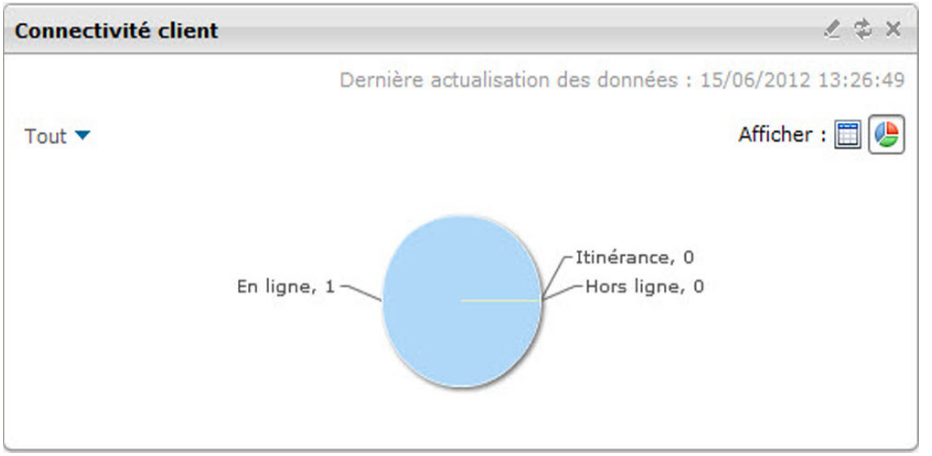


FIGURE 2-7. Widget Connectivité du client affichant un graphique circulaire

Widget de détection des risques liés à la sécurité

Le widget **Détection des risques liés à la sécurité** affiche le nombre de risques liés à la sécurité et d'ordinateurs infectés.

FIGURE 2-8. Widget de détection des risques liés à la sécurité

Si le nombre d'ordinateurs infectés est égal ou supérieur à 1, vous pouvez cliquer sur le nombre afin d'afficher les ordinateurs infectés dans l'arborescence des clients. Vous pouvez exécuter des tâches pour ces clients sur ces ordinateurs ou modifier leurs paramètres.

Widget Épidémies

Le widget **Épidémie** affiche l'état de toute épidémie virale actuelle, ainsi que la dernière alerte d'épidémie.

FIGURE 2-9. Widget Épidémies

Dans ce widget, vous pouvez effectuer les actions suivantes :

- Consultez les informations détaillées sur une épidémie en cliquant le lien Date/ Heure de l'alerte.
- Dès qu'OfficeScan détecte une épidémie, réinitialisez l'état des informations d'alerte d'épidémie et appliquez immédiatement les mesures de prévention d'épidémie. Pour plus d'informations sur l'application des mesures de prévention des épidémies, voir *Stratégies de prévention des épidémies à la page 6-104*.
- Cliquez sur **Afficher les statistiques du Top 10 des risques de sécurité** afin d'afficher les risques liés à la sécurité les plus courants, les ordinateurs comptant le

plus grand nombre de risques et les sources d'infections principales. Un nouvel écran s'affiche.

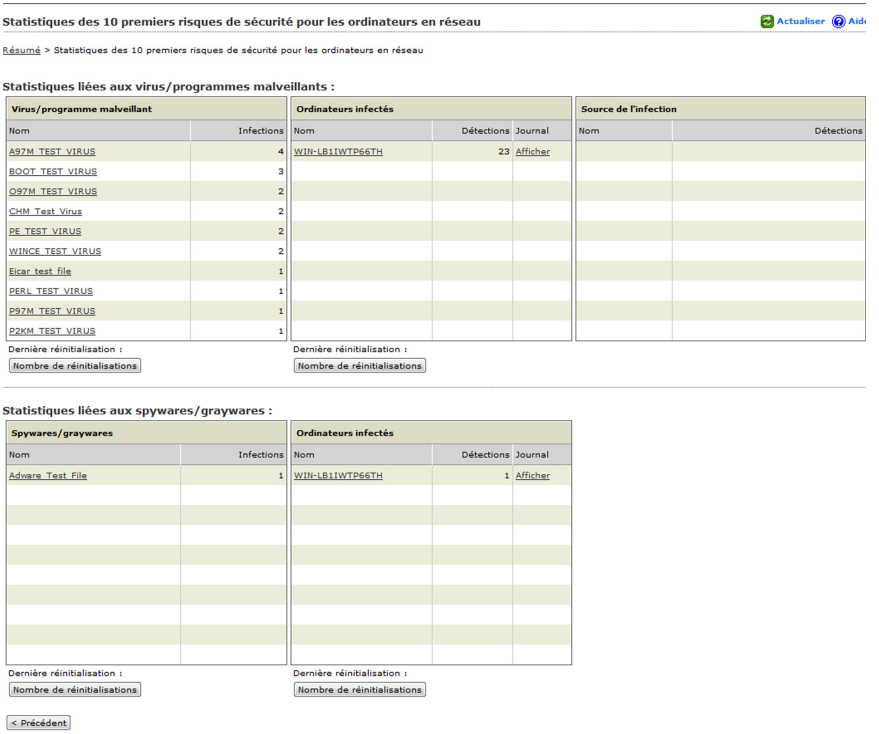


FIGURE 2-10. Écran des statistiques du Top 10 des risques de sécurité

Sur l'écran des **statistiques du Top 10 des risques de sécurité**, vous pouvez :

- Consulter des informations détaillées sur un risque de sécurité en cliquant sur le nom de ce risque.
- Consulter l'état général d'un ordinateur particulier en cliquant sur le nom de cet ordinateur.

- Consulter les journaux de risques de sécurité relatifs à cet ordinateur en cliquant sur le bouton **Afficher** correspondant au nom de l'ordinateur.
- Réinitialiser les statistiques dans chaque tableau en cliquant sur **Réinitialiser nombre**.

Widget Mises à jour du client

Le widget **Mises à jour du client** affiche les composants et programmes protégeant vos ordinateurs en réseau des risques liés à la sécurité.

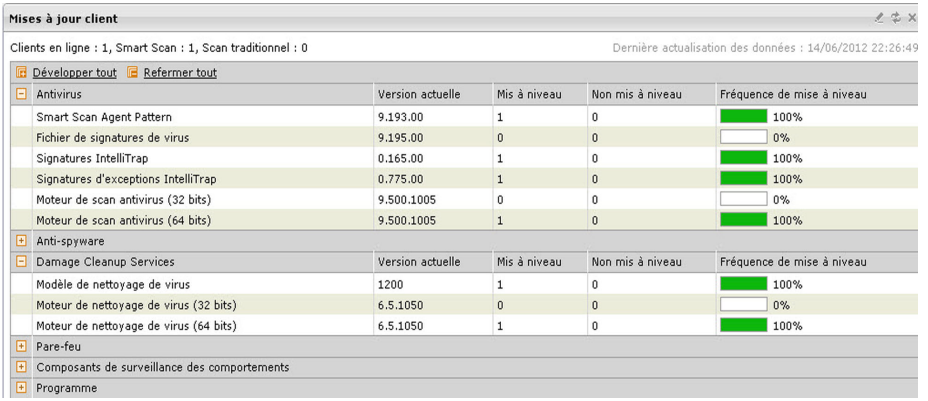

Mises à jour client
Clients en ligne : 1, Smart Scan : 1, Scan traditionnel : 0
Dernière actualisation des données : 14/06/2012 22:26:49
Développer tout
Refermer tout
Antivirus | Version actuelle | Mis à niveau | Non mis à niveau | Fréquence de mise à niveau
Smart Scan Agent Pattern | 9.193.00 | 1 | 0 | 100%
Fichier de signatures de virus | 9.195.00 | 0 | 0 | 0%
Signatures IntelliTrap | 0.165.00 | 1 | 0 | 100%
Signatures d'exceptions IntelliTrap | 0.775.00 | 1 | 0 | 100%
Moteur de scan antivirus (32 bits) | 9.500.1005 | 0 | 0 | 0%
Moteur de scan antivirus (64 bits) | 9.500.1005 | 1 | 0 | 100%
Anti-spyware
Damage Cleanup Services | Version actuelle | Mis à niveau | Non mis à niveau | Fréquence de mise à niveau
Modèle de nettoyage de virus | 1200 | 1 | 0 | 100%
Moteur de nettoyage de virus (32 bits) | 6.5.1050 | 0 | 0 | 0%
Moteur de nettoyage de virus (64 bits) | 6.5.1050 | 1 | 0 | 100%
Pare-feu
Composants de surveillance des comportements
Programme

FIGURE 2-11. Widget Mises à jour du client

Dans ce widget, vous pouvez effectuer les actions suivantes :

- Affichez la version actuelle de chaque composant.
- Sous la colonne **Obsolète**, affichez le nombre de clients avec des composants obsolètes. Si certains clients ont besoin d'être mis à jour, cliquez sur le lien numéroté pour démarrer cette mise à jour.
- Pour chaque programme, vous pouvez consulter les clients n'ayant pas été mis à niveau en cliquant sur le lien numéroté correspondant au programme.

Remarque

Pour mettre à niveau Cisco Trust Agent, accédez à **Cisco NAC** > **Déploiement de l'agent**.

Widget Mashup d'OfficeScan et des plugiciels

Le widget **Mashup d'OfficeScan et des plugiciels** combine les données des clients OfficeScan et des programmes de plug-in installés, puis présente les données dans l'arborescence des clients. Ce widget vous aide à évaluer rapidement la couverture de protection sur les clients et réduit le temps nécessaire à la gestion de chaque programme de plug-in.

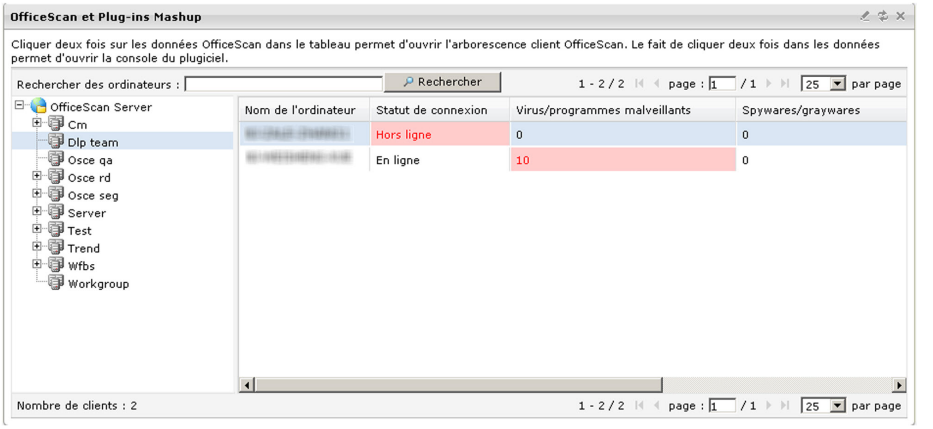


FIGURE 2-12. Widget Mashup d'OfficeScan et des plugiciels

Ce widget affiche les données pour les programmes de plug-in suivants :

- Intrusion Defense Firewall
- Trend Micro Virtual Desktop Support

Ces programmes de plug-in doivent être activés pour que le widget de mashup affiche les données. Mettez les programmes de plug-in à niveau si des versions plus récentes sont disponibles.

Dans ce widget, vous pouvez effectuer les actions suivantes :

- Choisissez les colonnes s'affichant dans l'arborescence des clients. Cliquez sur l'icône Modifier ( ) dans le coin supérieur droit du widget, puis sélectionnez les colonnes s'affichant sur l'écran.

TABLEAU 2-6. Colonnes Mashup d'OfficeScan et des plugiciels

NOM DE COLONNE	DESCRIPTION
Nom de l'ordinateur	Nom du point final Cette colonne est toujours disponible et ne peut être supprimée.
Hiérarchie des domaines	Le domaine du point final dans l'arborescence des clients OfficeScan
État de la connexion	La connectivité du client OfficeScan avec son serveur OfficeScan parent
Virus/programmes malveillants	Le nombre de virus et programmes malveillants détectés par le client OfficeScan
Spyware/Grayware	Le nombre de spywares et graywares détectés par le client OfficeScan
Prise en charge de VDI	Indique si le point final est une machine virtuelle ou non
Profil sécurité d'IDF	Consultez la documentation IDF pour plus d'informations sur ces colonnes et sur les données qu'elles présentent.
Pare-feu IDF	
État IDF	
DPI IDF	

- Double-cliquez sur les données du tableau. Si vous double-cliquez sur les données OfficeScan, l'arborescence des clients OfficeScan s'affiche. Si vous double-cliquez sur les données d'un programme de plug-in (à l'exception des données de la colonne **Prise en charge de VDI**), l'écran principal de ce programme s'affiche.
- Utilisez l'option de recherche pour trouver chaque point final. Vous pouvez saisir un nom d'hôte en totalité ou de façon partielle.

Widget Incidents majeurs de prévention contre la perte de données

Ce widget est disponible uniquement si vous activez la protection des données OfficeScan.

Ce widget affiche le nombre de transmissions d'actifs numériques, quelle que soit l'action (bloquée ou ignorée).

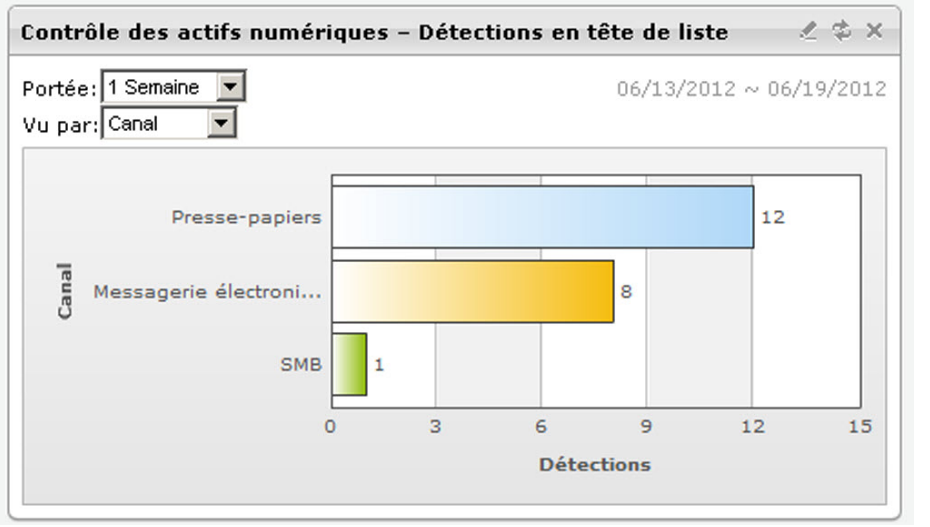


FIGURE 2-13. Widget Incidents majeurs de prévention contre la perte de données

Pour afficher les données :

1. Sélectionnez une période de temps pour les détections. Choisissez parmi :
   - **Aujourd'hui**: Détections durant les dernières 24 heures, en incluant l'heure actuelle
   - **1 semaine**: Détections durant les 7 derniers jours, en incluant le jour actuel
   - **2 semaines**: Détections durant les 14 derniers jours, en incluant le jour actuel
   - **1 mois**: Détections durant les 30 derniers jours, en incluant le jour actuel
2. Après avoir sélectionné la période de temps, choisissez parmi :

- **Utilisateur** : Utilisateurs transmettant le plus souvent des actifs numériques
- **Canal** : canaux les plus souvent utilisés afin de transmettre les actifs numériques
- **modèle** : modèles d'actifs numériques ayant déclenché la plupart des détections
- **Ordinateur** : Ordinateurs ayant transmis le plus souvent des actifs numériques

Remarque

Ce widget affiche un maximum de 10 utilisateurs, canaux, modèles ou ordinateurs.

Widget Incidents de prévention contre la perte de données dans le temps

Ce widget est disponible uniquement si vous activez la protection des données OfficeScan.

Ce widget affiche le nombre de transmissions d'actifs numériques pendant une période donnée. Les transmissions comprennent celles qui sont bloquées ou ignorées (autorisées).

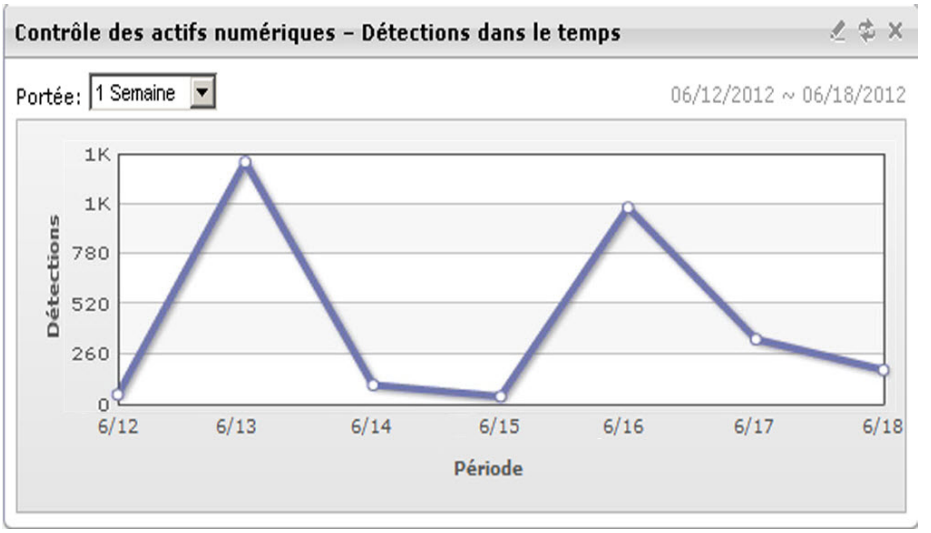


FIGURE 2-14. Widget Incidents de prévention contre la perte de données dans le temps

Pour afficher les données, sélectionnez une période de temps pour les détections. Choisissez parmi :

- **Aujourd'hui** : détections durant les dernières 24 heures, en incluant l'heure actuelle
- **1 semaine** : détections durant les 7 derniers jours, en incluant le jour actuel
- **2 semaines**: Détections durant les 14 derniers jours, en incluant le jour actuel
- **1 mois**: Détections durant les 30 derniers jours, en incluant le jour actuel

Widget Sources majeures des menaces selon la réputation des sites Web

Ce widget affiche le nombre total de détections de menaces liées à la sécurité effectuées par les services de réputation de sites Web. Les informations sont affichées sur une carte

du monde, en fonction de la localisation géographique. Pour obtenir de l'aide sur l'utilisation de ce widget, cliquez sur le bouton Aide (?) dans la partie supérieure du widget.

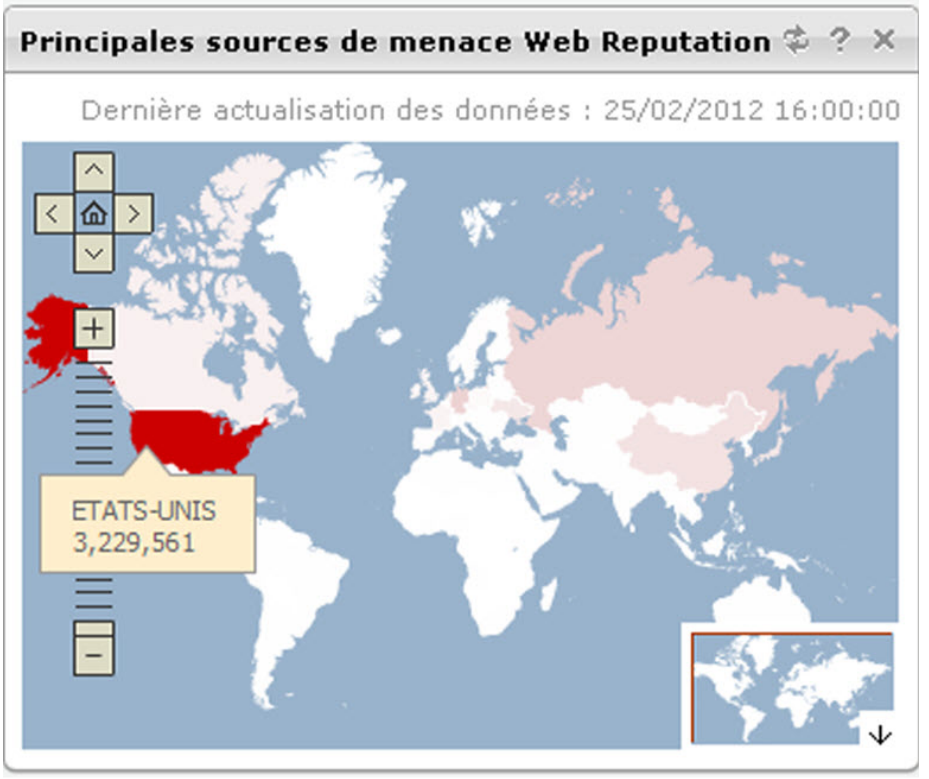


FIGURE 2-15. Widget Sources majeures des menaces selon la réputation des sites Web

Widget Utilisateurs les plus menacés selon la réputation des sites Web

Ce widget affiche le nombre d'utilisateurs infectés par des adresses URL malveillantes détectées par les services de réputation de sites Web. Les informations sont affichées sur une carte du monde, en fonction de la localisation géographique. Pour obtenir de l'aide

sur l'utilisation de ce widget, cliquez sur le bouton Aide (?) dans la partie supérieure du widget.

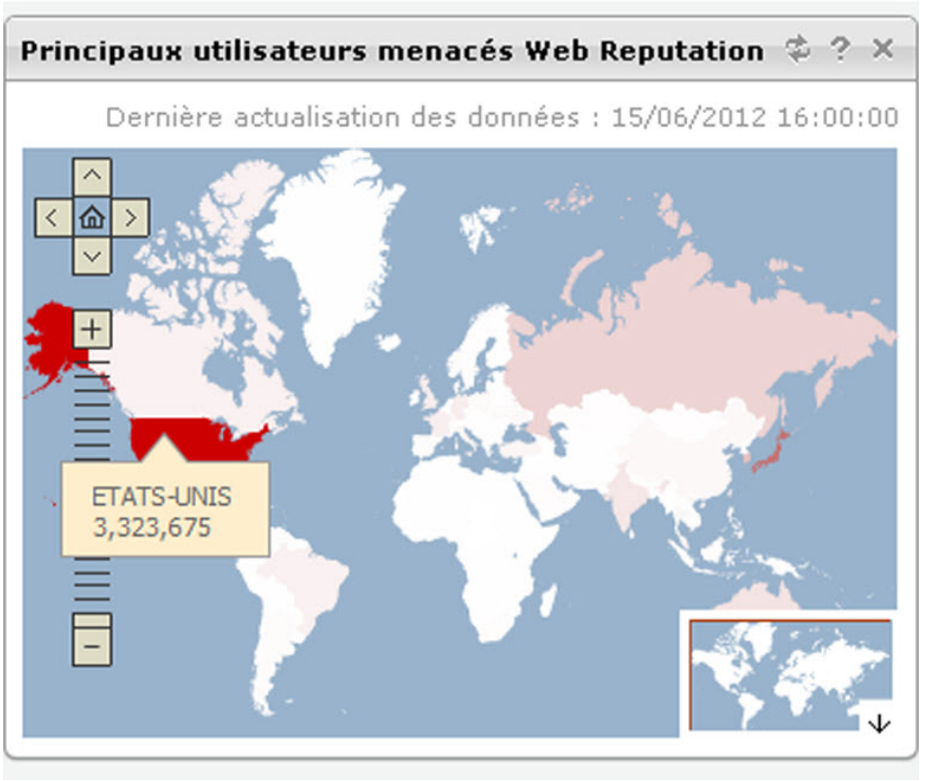


FIGURE 2-16. Widget Utilisateurs les plus menacés selon la réputation des sites Web

Widget Carte des menaces de File Reputation

Ce widget affiche le nombre total de détections de menaces liées à la sécurité effectuées par les services de file reputation. Les informations sont affichées sur une carte du monde, en fonction de la localisation géographique. Pour obtenir de l'aide sur

l'utilisation de ce widget, cliquez sur le bouton Aide (?) dans la partie supérieure du widget.

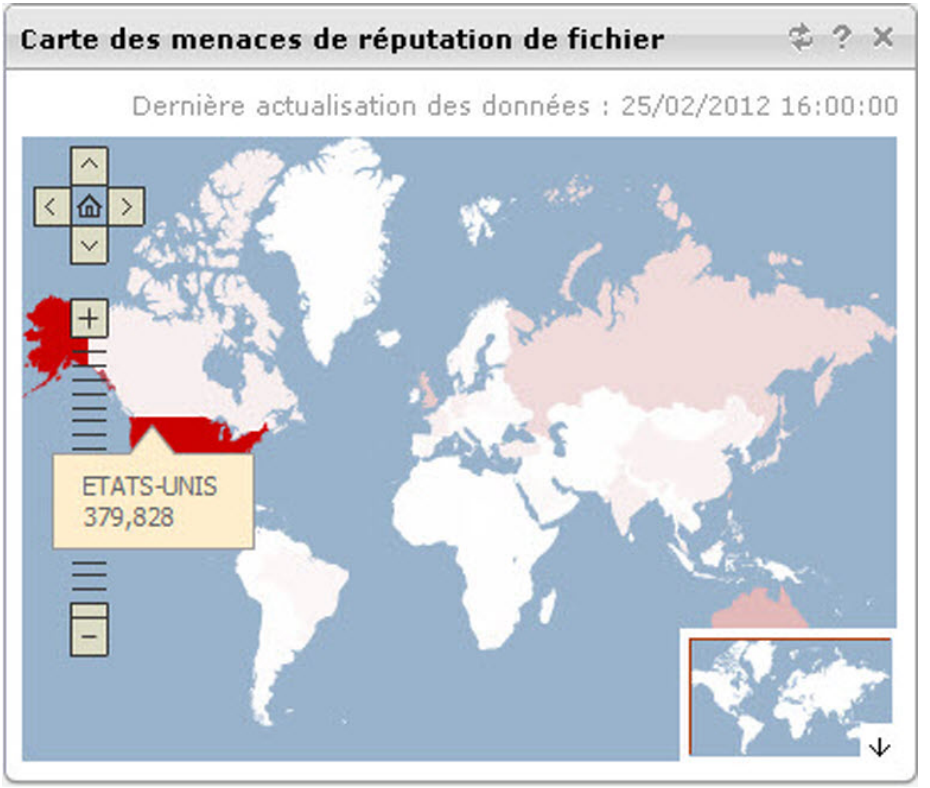


FIGURE 2-17. Widget Carte des menaces de File Reputation

Intégration d'Active Directory

Intégrez OfficeScan à votre structure Microsoft™ Active Directory™ pour gérer les clients OfficeScan plus efficacement, affectez des autorisations sur la console Web à l'aide de comptes Active Directory et déterminez les clients ne possédant pas de logiciel de sécurité installé. Tous les utilisateurs du domaine réseau peuvent bénéficier d'un accès

sécurisé à la console OfficeScan. Vous pouvez également affecter un accès limité à certains utilisateurs, même s'ils appartiennent à un autre domaine. Le processus d'authentification et la clé de chiffrement permettent de valider les informations d'authentification des utilisateurs.

Active Directory vous permet de tirer pleinement parti des fonctionnalités suivantes :

- **Role-based administration (Administration basée sur les rôles)** : affectez des responsabilités administratives spécifiques aux utilisateurs en leur accordant un accès à la console du produit à l'aide de leurs comptes Active Directory. Pour obtenir des informations détaillées, voir *Administration basée sur les rôles à la page 12-2*.
- **Groupes de clients personnalisés** : utilisez Active Directory ou des adresses IP pour regrouper manuellement des clients et les mapper sur des domaines de l'arborescence client OfficeScan. Pour obtenir des informations détaillées, voir *Regroupement automatique de clients à la page 2-47*.
- **Gestion des serveurs externes** : assurez-vous que les ordinateurs du réseau qui ne sont pas gérés par le serveur OfficeScan respectent les consignes de sécurité de votre société. Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les points finaux non gérés à la page 13-71*.

Synchronisez manuellement ou périodiquement la structure Active Directory avec le serveur OfficeScan pour garantir la cohérence des données. Pour obtenir des informations détaillées, voir *Synchronisation des données avec les domaines Active Directory à la page 2-30*.

Intégration d'Active Directory dans OfficeScan

Tâche

1. Accédez à **Administration** > **Active Directory** > **Intégration d'Active Directory**.
2. Sous **Domaines Active Directory**, spécifiez le nom du domaine Active Directory.
3. Indiquez les informations d'identification que le serveur OfficeScan Server utilisera lors de la synchronisation des données avec le domaine Active Directory spécifié. Les informations d'identification sont requises si le serveur ne fait pas partie du

domaine. Sinon, les informations d'identification sont facultatives. Assurez-vous que ces informations d'identification n'expirent pas ou le serveur ne sera pas en mesure de synchroniser les données.

a. Cliquez sur **Entrez les informations d'authentification du domaine**.

b. Dans la fenêtre contextuelle qui s'affiche, entrez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur peut être spécifié en utilisant l'un des formats suivants :

- `Domaine\Nom d'utilisateur`
- `nomdutilisateur@domaine`

c. Cliquez sur **Enregistrer**.

4. Cliquez sur le bouton (+) pour ajouter des domaines. Spécifiez les informations d'authentification de domaine pour les domaines ajoutés si nécessaire.

5. Cliquez sur le bouton (-) pour supprimer des domaines.

6. Spécifiez les paramètres de chiffrement si vous avez indiqué des informations d'identification de domaine. Par mesure de sécurité, OfficeScan chiffre les informations d'identification que vous avez spécifiées avant de les enregistrer dans la base de données. Lorsqu'OfficeScan synchronise les données avec l'un des domaines spécifiés, il utilise une clé de chiffrement pour déchiffrer les informations d'identification du domaine.

a. Rendez-vous à la section **Paramètres de chiffrement pour les informations d'identification du domaine**.

b. Entrez une clé d'encodage qui ne dépasse pas 128 caractères.

c. Indiquez un fichier dans lequel enregistrer la clé d'encodage. Vous pouvez choisir un format de fichier courant, comme `.txt`. Entrez le nom et le chemin d'accès complets du fichier, comme `C:\AD_Encryption\EncryptionKey.txt`.

AVERTISSEMENT!

Si le fichier est supprimé ou si le chemin d'accès est modifié, OfficeScan ne pourra pas synchroniser les données avec l'ensemble des domaines spécifiés.

7. Choisissez l'une des options suivantes :

   - **Enregistrer** : Enregistrez les paramètres uniquement. La synchronisation des données pouvant accaparer les ressources du réseau, vous pouvez choisir d'enregistrer les paramètres uniquement et de synchroniser plus tard, en heures creuses.
   - **Enregistrer et synchroniser**: enregistre les paramètres et synchronise les données avec les domaines Active Directory.

8. Programmez des synchronisations périodiques. Pour obtenir des informations détaillées, voir *Synchronisation des données avec les domaines Active Directory à la page 2-30*.

Synchronisation des données avec les domaines Active Directory

Synchronisez régulièrement les données avec les domaines Active Directory pour maintenir l'arborescence du client d'OfficeScan à jour et interroger les clients non gérés.

Synchronisation manuelle des données avec les domaines Active Directory

Tâche

1. Accédez à **Administration** > **Active Directory** > **Intégration d'Active Directory**.
2. Vérifiez que les informations d'authentification du domaine et les paramètres de chiffrement n'ont pas changé.
3. Cliquez sur **Enregistrer et synchroniser**.

Synchronisation automatique des données avec les domaines Active Directory

Tâche

1. Accédez à **Administration** > **Active Directory** > **Synchronisation programmée**.
2. Sélectionnez **Activer la synchronisation programmée d'Active Directory**.
3. Programmez la synchronisation.

Remarque

Pour des synchronisations quotidiennes, hebdomadaires et mensuelles, la période correspond au nombre d'heures pendant lesquelles OfficeScan synchronise Active Directory avec le serveur OfficeScan.

4. Cliquez sur **Enregistrer**.

L'arborescence des clients OfficeScan

L'arborescence client OfficeScan permet d'afficher tous les clients (regroupés dans les *Domaines OfficeScan à la page 2-44*) que le serveur gère actuellement. Les clients sont regroupés en domaines afin de vous permettre de configurer, gérer et appliquer simultanément la même configuration à tous les membres du domaine.

L'arborescence des clients s'affiche dans le cadre principal lorsque vous cliquez sur certaines fonctions dans le menu principal.

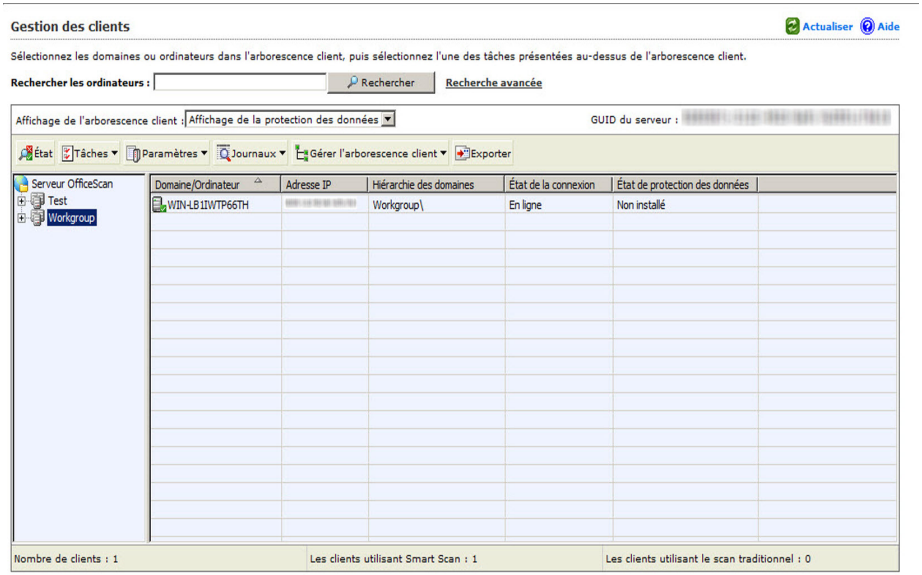


FIGURE 2-18. arborescence des clients OfficeScan

Tâches générales dans l'arborescence des clients

Certaines tâches que vous pouvez effectuer lorsque l'arborescence des clients est affichée sont décrites ci-dessous :

Tâche

- Cliquez sur l'icône du domaine racine ( ) pour sélectionner tous les domaines et clients. Lorsque vous sélectionnez l'icône de domaine se trouvant à la racine, puis choisissez une tâche au-dessus de l'arborescence des clients, un écran permettant de configurer les paramètres s'affiche. Sur l'écran, choisissez parmi les options générales suivantes :
  - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les

domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

- Pour sélectionner plusieurs domaines ou clients adjacents :
  - Dans le panneau de droite, sélectionnez le premier domaine, appuyez et maintenez la touche MAJ enfoncée, puis cliquez sur le dernier domaine ou client de la plage.
- Pour sélectionner plusieurs domaines ou clients n'étant pas à la suite les uns des autres, appuyez et maintenez la touche CTRL enfoncée, puis cliquez sur les domaines ou clients à sélectionner.
- Recherchez un client à gérer en spécifiant son nom dans le champ **Rechercher les ordinateurs**. Le domaine s'affiche, avec la liste de tous les clients qu'il contient, le nom du client spécifié étant mis en évidence. Pour passer au client suivant, cliquez à nouveau sur **Rechercher**. Pour disposer de plus d'options de recherche, cliquez sur **Recherche avancée**.

Remarque

Les adresses IPv6 ou IPv4 ne peuvent pas être indiquées dans le cadre d'une recherche de clients spécifiques. Utilisez la recherche avancée pour faire une recherche à partir d'une adresse IPv4 ou IPv6. Pour obtenir des informations détaillées, voir *Options de recherche avancée à la page 2-34*.

- Après avoir sélectionné un domaine, le tableau de l'arborescence des clients se déploie pour montrer les clients appartenant au domaine, ainsi que toutes les colonnes contenant des informations importantes pour chaque client. Pour afficher uniquement quelques colonnes connexes, sélectionnez un élément dans l'affichage de l'arborescence du client.
  - **Afficher tout** : affiche toutes les colonnes
  - **Mise à jour** : affiche tous les composants et programmes
  - **Affichage antivirus** : affiche les composants antivirus

  - **Affichage antispyware :** affiche les composants anti-spyware
  - **Affichage de la protection des données** : indique l'état du module Protection des données sur les clients
  - **Pare-feu** : affiche les composants de pare-feu
  - **Affichage Smart protection** : affiche la méthode de scan utilisée par les clients (scan traditionnel ou Smart Scan) et les composants Smart Protection
  - **Agent de mise à jour** : affiche des informations pour tous les agents de mise à jour gérés par le serveur OfficeScan
- Vous pouvez organiser autrement les colonnes en faisant glisser les titres des colonnes à d'autres endroits de l'arborescence des clients. OfficeScan sauvegarde automatiquement les nouvelles positions de colonne.
- Triez les clients en fonction des informations de colonne en cliquant sur le nom de la colonne.
- Actualisez l'arborescence client en cliquant sur l'icône d'actualisation ( ).
- Affichez les statistiques relatives aux clients sous l'arborescence des clients, telles que le nombre de clients Smart Scan et le nombre de clients de scan traditionnel.

Options de recherche avancée

Recherchez les clients en fonction des critères suivants :

Tâche

- **Éléments de base** : comprend des informations de base sur les ordinateurs, telles que l'adresse IP, le système d'exploitation, le domaine, l'adresse MAC, la méthode de scan et le statut de réputation de sites Web.
  - La recherche par plage d'adresses IPv4 requiert une partie d'une adresse IP commençant par le premier octet. La fonction de recherche localise tous les ordinateurs dont l'adresse IP contient l'élément saisi. Par exemple, si vous tapez 10.5, vous trouverez tous les ordinateurs dont l'adresse IP est incluse dans une plage allant de 10.5.0.0 à 10.5.255.255.

  - La recherche par plage d'adresses IPv6 requiert un préfixe et une longueur.
  - La recherche par adresse MAC requiert une plage d'adresses MAC en notation hexadécimale, par exemple 000A1B123C12.

- **Versions du composant** : cochez la case en regard du nom de composant, définissez le critère en sélectionnant **Antérieur à** ou **antérieur ou égal à**, puis entrez un numéro de version. Le numéro de version actuel s'affiche par défaut.
- **État** : inclut les paramètres client

Cliquez sur **Rechercher** après avoir spécifié les critères de recherche. Une liste des noms d'ordinateurs répondant aux critères s'affiche dans l'arborescence du client.

Tâches spécifiques dans l'arborescence des clients

L'arborescence des clients s'affiche lorsque vous accédez à certains écransde la console Web. Des éléments de menu propres à l'écran via lequel vous accédez apparaissent au-dessus de l'arborescence des clients. Ils vous permettent de réaliser certaines tâches, comme par exemple la configuration de paramètres client ou l'initialisation de tâches client. Pour effectuer une tâche quelconque, commencez par sélectionner la cible de la tâche (soit le domaine racine, ce qui entraînera l'application des paramètres à tous les clients, soit un ou plusieurs domaines, ou encore un ou plusieurs clients), puis sélectionnez un élément de menu.

Les écrans suivants affichent l'arborescence client :

- *Écran Paramètres clients généraux à la page 2-36*
- *Écran Prévention des épidémies à la page 2-39*
- *Écran Mise à jour des composants pour les ordinateurs en réseau à la page 2-40*
- *Écran Rétrograder à la page 2-41*
- *Écran Journaux de risques de sécurité pour ordinateurs en réseau à la page 2-42*
- *Écran Déploiement de l'agent à la page 2-44*

Écran Paramètres clients généraux

Pour afficher cet écran, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux**.

Gérez les paramètres clients généraux dans l'écran **Paramètres clients généraux**.

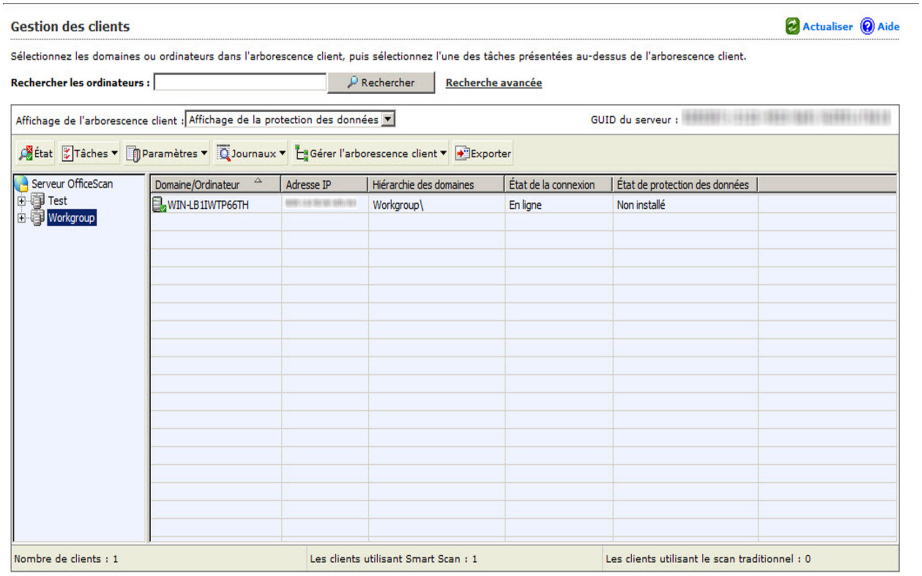


FIGURE 2-19. Écran Paramètres clients généraux

Le tableau suivant répertorie les tâches que vous pouvez effectuer :

TABLEAU 2-7. Tâches Paramètres clients généraux

BOUTON DE MENU	TÂCHE
État	Afficher les informations sur le client. Pour obtenir des informations détaillées, voir *Affichage des informations du client OfficeScan à la page 13-55*.

BOUTON DE MENU	TÂCHE
Tâches	• Exécuter un scan immédiat sur les ordinateurs clients. Pour obtenir des informations détaillées, voir *Exécution du scan immédiat à la page 6-25*. • Désinstaller le client. Pour obtenir des informations détaillées, voir *Désinstallation du client OfficeScan de la console Web à la page 4-71*. • Restaurer des spywares/graywares. Pour obtenir des informations détaillées, voir *Restauration des spywares/graywares à la page 6-51*.

BOUTON DE MENU	TÂCHE

Paramètres	• Configurer les paramètres de scan. Pour obtenir des informations détaillées, reportez-vous aux sections suivantes :
	  • *Méthodes de scan à la page 6-8*
	  • *Scan manuel à la page 6-18*
	  • *Scan en temps réel à la page 6-15*
	  • *Scan programmé à la page 6-20*
	  • *Scan immédiat à la page 6-23*
	• Configurer les paramètres de réputation de sites Web. Pour obtenir des informations détaillées, voir *Stratégies de réputation de sites Web à la page 10-3*.
	• Configurer les paramètres de surveillance des comportements. Pour obtenir des informations détaillées, voir *Surveillance des comportements à la page 7-2*.
	• Configurer les paramètres de contrôle des dispositifs. Pour obtenir des informations détaillées, voir *Contrôle des dispositifs à la page 8-2*.
	• Configurer les stratégies de prévention contre la perte de données. Pour obtenir des informations détaillées, voir *Configuration de la stratégie de prévention contre la perte de données à la page 9-50*.
	• Attribuer aux clients le rôle d'agent de mise à jour. Pour obtenir des informations détaillées, voir *Configuration de l'agent de mise à jour à la page 5-56*.
	• Configurer les privilèges et autres paramètres du client. Pour obtenir des informations détaillées, voir *Configuration des privilèges clients et autres paramètres à la page 13-90*.
	• Activer ou désactiver les services clients OfficeScan. Pour obtenir des informations détaillées, voir *Services du client OfficeScan à la page 13-7*.
	• Modifier la liste de spywares/graywares approuvés. Pour obtenir des informations détaillées, voir *Liste des spywares/graywares approuvés à la page 6-49*.
	• Importer et exporter les paramètres du client. Pour obtenir des informations détaillées, voir *Importation et exportation des paramètres du client à la page 13-55*.

BOUTON DE MENU	TÂCHE
Journaux	Afficher les journaux suivants : • Journaux de virus/programmes malveillants (pour plus d'informations, voir *Affichage des journaux de virus/programmes malveillants à la page 6-87*) • Journaux de spywares/graywares (pour plus d'informations, voir *Affichage des journaux de spywares/graywares à la page 6-94*) • Journaux de pare-feu (pour plus d'informations, voir *Journaux de pare-feu à la page 11-30*) • Journaux de réputation de sites Web (pour plus d'informations, voir *Journaux de réputation de sites Web à la page 10-11*) • Journaux de surveillance des comportements (pour plus d'informations, voir *Journaux de surveillance des comportements à la page 7-13*) • Journaux de contrôle des dispositifs (pour plus d'informations, voir *Journaux de contrôle des dispositifs à la page 8-17*) Suppression des journaux. Pour obtenir des informations détaillées, voir *Gestion du journal à la page 12-36*.
Gérer l'arborescence des clients	Gérer l'arborescence des clients. Pour obtenir des informations détaillées, voir *Tâches de regroupement de clients à la page 2-52*.
Exporter	Exporter une liste des clients dans un fichier au format (`.csv`).

Écran Prévention des épidémies

Pour afficher cet écran, accédez à **Ordinateurs en réseau** > **Prévention des épidémies**.

Indiquez et activez les paramètres de prévention des épidémies dans l'écran **Prévention des épidémies**. Pour obtenir des informations détaillées, voir *Configuration de la prévention des épidémies de risques liés à la sécurité à la page 6-103*.

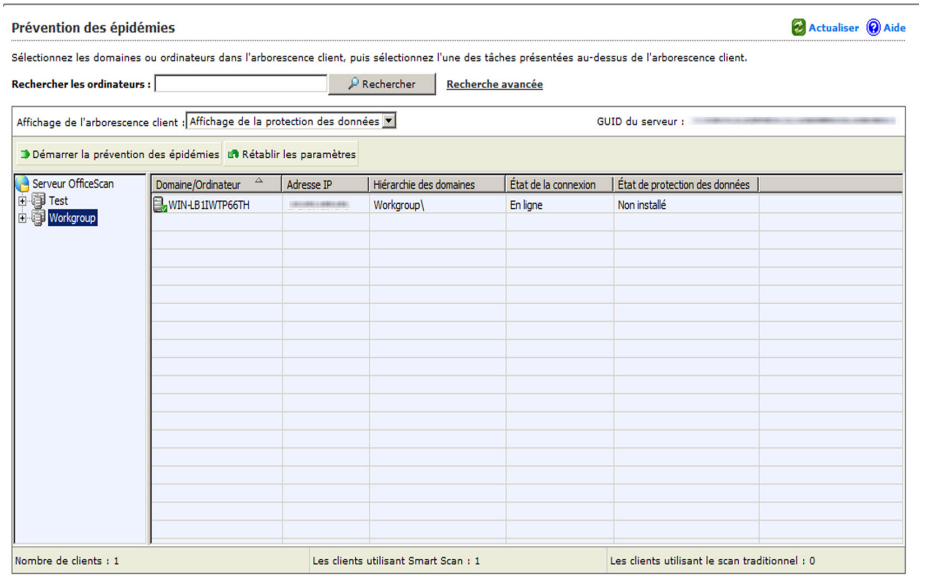


FIGURE 2-20. Écran Prévention des épidémies

Écran Mise à jour des composants pour les ordinateurs en réseau

Pour afficher cet écran, accédez à **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour manuelle**.. Cliquez sur **Sélectionner manuellement les clients**, puis cliquez sur **Sélectionner**.

Lancez la mise à jour manuelle à partir de l'écran **Mise à jour des composants pour les ordinateurs en réseau.** Pour obtenir des informations détaillées, voir *Mise à jour manuelle des clients OfficeScan à la page 5-44*.

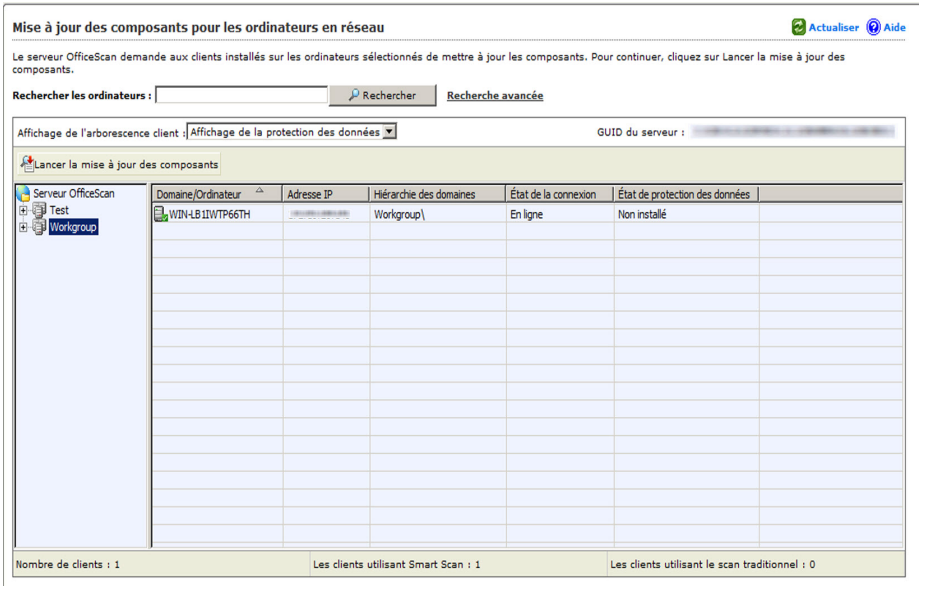

Mise à jour des composants pour les ordinateurs en réseau
Actualiser
Aide
Le serveur OfficeScan demande aux clients installés sur les ordinateurs sélectionnés de mettre à jour les composants. Pour continuer, cliquez sur Lancer la mise à jour des composants.
Rechercher les ordinateurs :
Rechercher
Recherche avancée
Affichage de l'arborescence client :
Affichage de la protection des données
GUID du serveur :
Lancer la mise à jour des composants
Serveur OfficeScan
Test
Workgroup
Domaine/Ordinateur
Adresse IP
Hiérarchie des domaines
État de la connexion
État de protection des données
WIN-LB1IWTP66TH
Workgroup\
En ligne
Non installé
Nombre de clients : 1
Les clients utilisant Smart Scan : 1
Les clients utilisant le scan traditionnel : 0

FIGURE 2-21. Écran Mise à jour des composants pour les ordinateurs en réseau

Écran Rétrograder

Pour afficher cet écran, accédez à **Mises à jour** > **Rétrograder**. Cliquez sur **Synchroniser avec le serveur**.

Rétrogradez les composants clients dans l'écran **Rétrograder**. Pour obtenir des informations détaillées, voir *Rétrogadation des composants pour les clients OfficeScan à la page 5-53*.

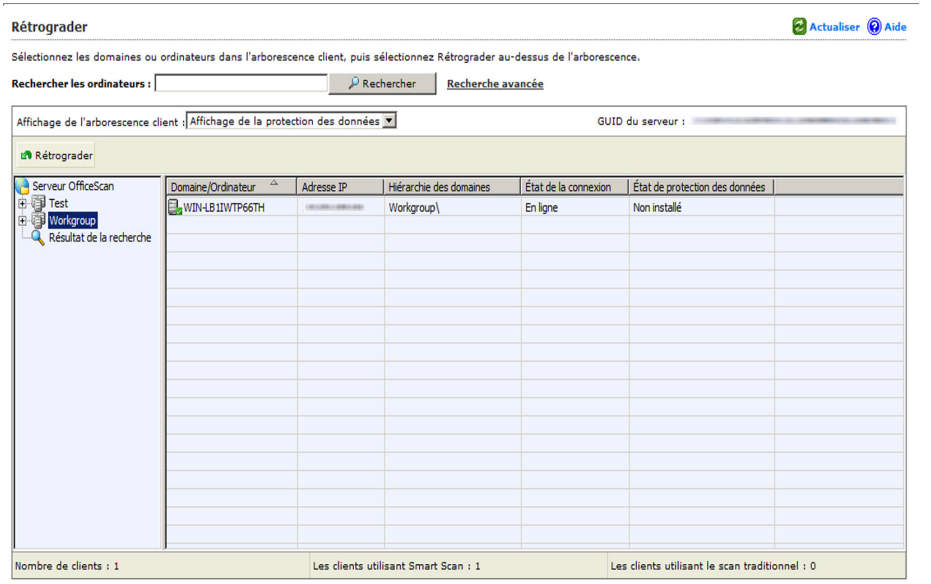


FIGURE 2-22. Écran Rétrograder

Écran Journaux de risques de sécurité pour ordinateurs en réseau

Pour afficher cet écran, accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité**.

Affichez et gérez les journaux dans l'écran **Journaux de risques de sécurité pour ordinateurs en réseau**.

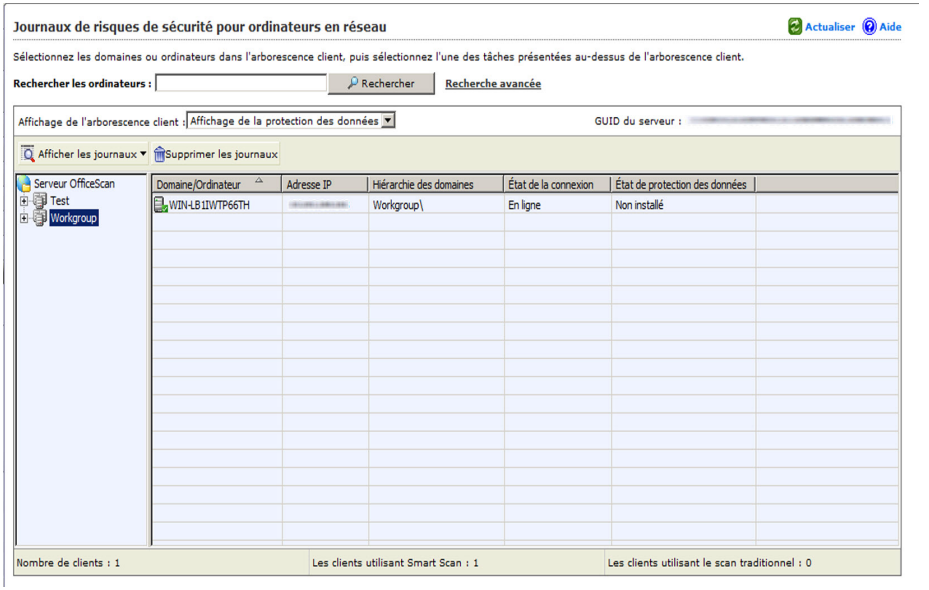


FIGURE 2-23. Écran Journaux de risques de sécurité pour ordinateurs en réseau

Effectuez les actions suivantes :

1. Afficher les journaux envoyés au serveur par les clients. Pour plus d'informations, voir :
   - *Affichage des journaux de virus/programmes malveillants à la page 6-87*
   - *Affichage des journaux de spywares/graywares à la page 6-94*
   - *Affichage des journaux du pare-feu à la page 11-31*
   - *Affichage de journaux de réputation de sites Web à la page 10-11*
   - *Affichage des journaux de surveillance des comportements à la page 7-13*
   - *Affichage des journaux de contrôle des dispositifs à la page 8-18*

- *Affichage des journaux de prévention contre la perte de données à la page 9-60*

2. Suppression des journaux. Pour obtenir des informations détaillées, voir *Gestion du journal à la page 12-36*.

Écran Déploiement de l'agent

Pour afficher cet écran, accédez à **Cisco NAC** > **Déploiement de l'agent**.

Si un serveur Policy Server a été configuré pour Cisco NAC, déployer Cisco Trust Agent (CTA) aux clients finaux dans l'écran **Déploiement de l'agent** Pour obtenir des informations détaillées, voir *Déploiement de Cisco Trust Agent à la page 15-30*.

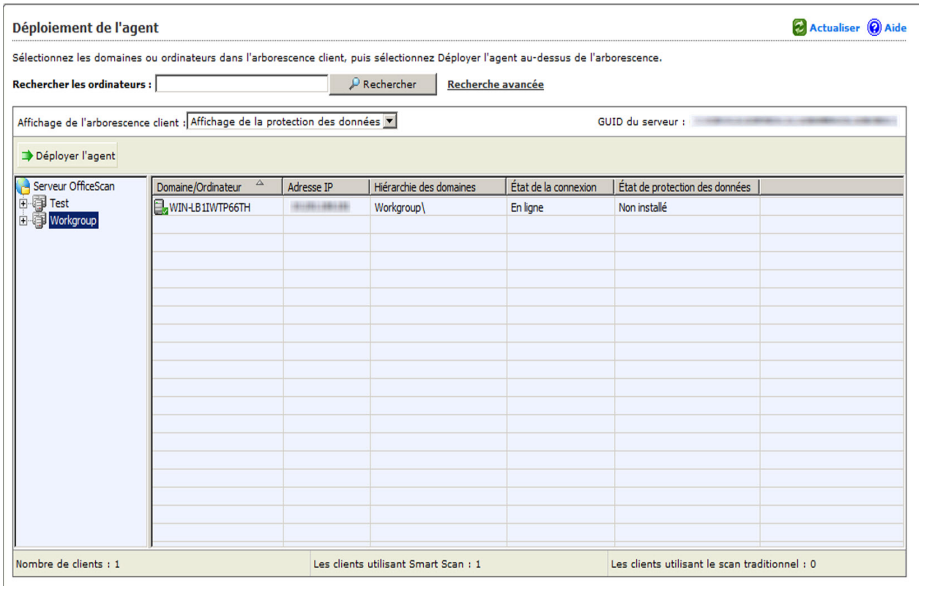


FIGURE 2-24. Écran Déploiement de l'agent

Domaines OfficeScan

Sous OfficeScan, un domaine est un groupe de clients partageant une configuration commune et exécutant des tâches similaires. En regroupant les clients en domaines, vous

pouvez configurer, gérer et appliquer la même configuration à tous les membres du domaine. Pour plus d'informations sur le regroupement de clients, reportez-vous à *Regroupement des clients à la page 2-45*.

Regroupement des clients

Utilisez le regroupement de clients pour créer manuellement ou automatiquement et gérer des domaines dans l'arborescence des clients OfficeScan.

Il est possible de regrouper les clients dans des domaines selon deux méthodes.

TABLEAU 2-8. Méthodes de regroupement des clients

MÉTHODE	REGROUPEMENT DES CLIENTS	DESCRIPTIONS
Manuelle	• Domaine NetBIOS • Domaine Active Directory • Domaine DNS	Le regroupement manuel de clients définit le domaine auquel un nouveau client installé doit appartenir. Lorsque le client apparaît dans l'arborescence des clients, vous pouvez le déplacer dans un autre domaine ou serveur OfficeScan. Le regroupement manuel de clients permet également de créer, de gérer et de supprimer des domaines de l'arborescence client. Pour obtenir des informations détaillées, voir *Regroupement manuel des clients à la page 2-46*.
Automatique	Groupes de clients personnalisés	Le regroupement automatique de clients s'appuie sur des règles pour trier des clients dans l'arborescence des clients. Après avoir défini les règles, vous pouvez accéder à l'arborescence des clients afin de trier manuellement les clients, d'autoriser OfficeScan à les trier automatiquement lorsqu'un événement particulier a lieu ou à des intervalles programmées. Pour obtenir des informations détaillées, voir *Regroupement automatique de clients à la page 2-47*.

Regroupement manuel des clients

OfficeScan n'utilise ce paramètre que lors de nouvelles installations de clients. Le programme d'installation vérifie le domaine réseau auquel appartient l'ordinateur cible. Si le nom de domaine existe déjà dans l'arborescence client, OfficeScan regroupe le client de l'ordinateur cible sous ce domaine et applique les paramètres configurés pour ce dernier. Si le nom de domaine n'existe pas, OfficeScan ajoute le domaine à l'arborescence des clients, regroupe le client sous ce domaine, puis applique les paramètres racine au domaine et au client.

Configuration du regroupement manuel de clients

Tâche

1. Accédez à **Ordinateurs en réseau** > **Regroupement des clients**.
2. Spécifiez la méthode de regroupement des clients :
   - Domaine NetBIOS
   - Domaine Active Directory
   - Domaine DNS
3. Cliquez sur **Enregistrer**.

Que faire ensuite

Pour gérer les domaines et les clients regroupés sous ces domaines, procédez comme suit :

- Ajouter un domaine
- Supprimer un domaine ou un client
- Renommer un domaine
- Déplacer un client vers un autre domaine

Pour obtenir des informations détaillées, voir *Tâches de regroupement de clients à la page 2-52*.

Regroupement automatique de clients

Le regroupement automatique de clients s'appuie sur des règles définies par les adresses IP ou les domaines Active Directory. Si une règle définit une adresse IP ou une plage d'adresses IP, le serveur OfficeScan regroupera un client avec une adresse IP correspondante à un domaine spécifique dans l'arborescence client. De plus, si une règle définit un ou plusieurs domaines Active Directory, le serveur OfficeScan regroupera un client appartenant à un domaine Active Directory particulier à un domaine spécifique dans l'arborescence client.

Les clients n'appliquent qu'une règle à la fois. Attribuez des priorités aux règles de manière à ce que, si un client respecte plus d'une règle, la règle dont la priorité est la plus élevée s'applique.

Configuration du regroupement automatique de clients

Tâche

1. Accédez à **Ordinateurs en réseau** > **Regroupement des clients**.
2. Allez dans la section **Regroupement des clients** et sélectionnez **Groupes de clients personnalisés**.
3. Allez dans la section **Regroupement automatique de clients**.
4. Pour commencer à créer des règles, cliquez sur **Ajouter**, puis sélectionnez **Active Directory** ou **Adresse IP**.
   - Si vous avez sélectionné **Active Directory**, consultez les instructions de configuration dans *Définir une règle de regroupement de clients par domaines Active Directory à la page 2-49*.
   - Si vous avez sélectionné **Adresse IP**, consultez les instructions de configuration dans *Définir une règle de regroupement de clients par adresses IP à la page 2-50*.
5. Si vous avez créé plus d'une règle, attribuez une priorité aux règles en exécutant ces étapes :
   a. Sélectionnez une règle.

b. Sous la colonne **Priorité de regroupement**, cliquez sur l'une des flèches pour déplacer la règle vers le haut ou le bas de la liste. Le numéro ID de la règle change pour indiquer cette nouvelle position.

6. Pour utiliser les règles lors du tri des clients :

   a. Cochez les cases pour les règles que vous souhaitez utiliser.

   b. Assurez-vous que les règles sont activées. Sous la colonne État, une coche verte ( ) devrait apparaître. Si une coche « x » rouge ( ) apparaît, cliquez sur l'icône pour activer la règle et faire passer l'icône en vert.

Remarque

Si vous ne cochez pas la case pour une règle ou si vous désactivez une règle, cette dernière ne sera pas utilisée lors du tri des clients dans l'arborescence client. Par exemple, si la règle indique qu'un client doit aller dans un nouveau domaine, le client restera dans son domaine actuel.

7. Spécifiez un calendrier de tri dans la section **Création de domaine programmée**.

   a. Sélectionnez **Activer la création de domaine programmée**.

   b. Spécifiez le programme sous **Création de domaine programmée**.

8. Sélectionnez l'une des options suivantes :

   - **Enregistrer et créer le domaine maintenant** : Choisissez cette option si vous avez spécifié de nouveaux domaines dans *Définir une règle de regroupement de clients par adresses IP à la page 2-50*, étape 7 ou dans *Définir une règle de regroupement de clients par domaines Active Directory à la page 2-49*, étape 7.

   - **Enregistrer** : Choisissez cette option si vous n'avez pas spécifié de nouveaux domaines ou si vous souhaitez créer de nouveaux domaines uniquement lorsque le tri client est actif.

Remarque

Le tri de clients ne débutera pas après l'exécution de cette étape.

9. Pour trier des clients immédiatement, allez dans l'arborescence client et triez-les. Pour obtenir des informations détaillées, voir *Tri des clients à la page 2-55*. Si vous

avez configuré un calendrier de tri à l'étape 6, le tri débutera au jour et à l'heure indiqués. OfficeScan exécutera également une tâche de tri lorsque les éléments suivants surviennent :

- Un client est installé.
- Un client se recharge.
- L'adresse IP d'un client change.
- Un utilisateur client active ou désactive le mode itinérant.

Définir une règle de regroupement de clients par domaines Active Directory

Assurez-vous que vous avez configuré les paramètres d'intégration d'Active Directory avant d'exécuter les étapes de la procédure ci-dessous. Pour obtenir des informations détaillées, voir *Intégration d'Active Directory à la page 2-27*.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Regroupement des clients**.
2. Allez dans la section **Regroupement des clients** et sélectionnez **Groupes de clients personnalisés**.
3. Allez dans la section **Regroupement automatique de clients**.
4. Cliquez sur **Ajouter**, puis sélectionnez **Active Directory**.

   Un nouvel écran s'affiche.
5. Sélectionnez **Autoriser le groupage**.
6. Indiquez un nom pour la règle.
7. Sous **Source d'Active Directory**, sélectionnez le(s) domaine(s) ou sous-domaine(s) Active Directory.
8. Sous **Arborescence client**, sélectionnez un domaine OfficeScan existant sur lequel les domaines Active Directory mappent. Si le domaine OfficeScan souhaité n'existe pas, effectuez les étapes suivantes :

a. Passez la souris sur un domaine OfficeScan particulier et cliquez sur l'icône d'ajout de domaine. Dans l'exemple ci-dessous, le nouveau domaine sera ajouté sous le domaine racine OfficeScan.

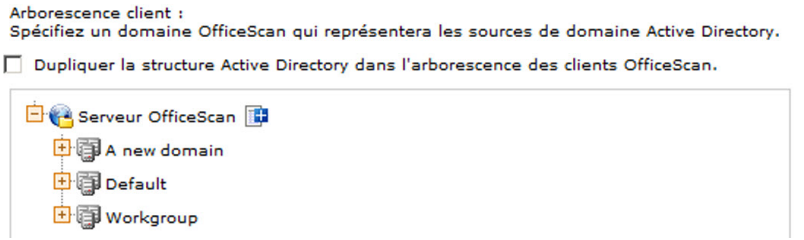

Arborescence client :
Spécifiez un domaine OfficeScan qui représentera les sources de domaine Active Directory.
Dupliquer la structure Active Directory dans l'arborescence des clients OfficeScan.
Serveur OfficeScan
A new domain
Default
Workgroup

FIGURE 2-25. Icône d'ajout de domaine

b. Saisissez le nom de domaine dans la zone de texte prévue à cet effet.

c. Cliquez sur la coche en regard de la zone de texte. Le nouveau domaine est ajouté et est automatiquement sélectionné.

9. (Facultatif) Sélectionnez **Dupliquer la structure Active Directory dans l'arborescence client OfficeScan**. Cette option duplique la hiérarchie des domaines Active Directory sélectionnés dans le domaine OfficeScan sélectionné.

10. Cliquez sur **Enregistrer**.

Définir une règle de regroupement de clients par adresses IP

Créez des groupes de clients personnalisés en utilisant les adresses IP réseau pour trier les clients dans l'arborescence client OfficeScan. Cette fonctionnalité peut aider les administrateurs à organiser l'arborescence des clients OfficeScan avant que le client ne s'enregistre auprès du serveur OfficeScan.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Regroupement des clients**.

2. Allez dans la section **Regroupement des clients** et sélectionnez **Groupes de clients personnalisés**.

3. Allez dans la section **Regroupement automatique de clients**.

4. Cliquez sur **Ajouter**, puis sélectionnez **Adresse IP**.

   Un nouvel écran s'affiche.

5. Sélectionnez **Autoriser le groupage**.

6. Spécifiez un nom pour le regroupement.

7. Spécifiez l'un des éléments suivants :

   - Une adresse IPv4 ou IPv6 unique
   - Une plage d'adresse IPv4
   - Un préfixe et une longueur IPv6

Remarque

Si les adresses IPv4 et IPv6 d'un client double-pile appartiennent à deux groupes de clients distincts, le client sera regroupé sous le groupe IPv6. Si l'IPv6 est désactivée sur l'ordinateur hôte du client, ce dernier ira dans le groupe IPv4.

8. Sélectionnez le domaine OfficeScan sur lequel l'adresse IP ou la plage d'adresses IP est mappée. Si le domaine n'existe pas, effectuez ce qui suit :

   a. Passez la souris n'importe où sur l'arborescence client et cliquez sur l'icône d'ajout de domaine.

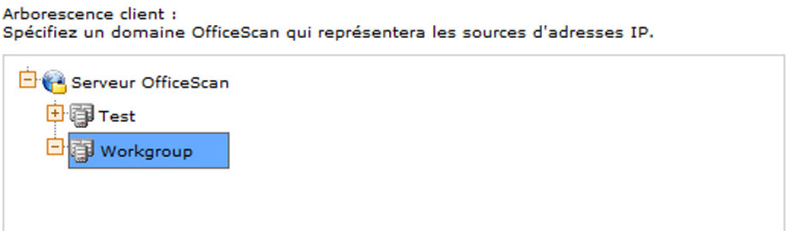


FIGURE 2-26. Icône d'ajout de domaine

   b. Saisissez le domaine dans la zone de texte prévue à cet effet.

   c. Cliquez sur la coche en regard de la zone de texte. Le nouveau domaine est ajouté et est automatiquement sélectionné.

9. Cliquez sur **Enregistrer**.

Tâches de regroupement de clients

Vous pouvez effectuer les tâches suivantes lors du regroupement de clients dans des domaines :

Regroupement manuel de clients :

- Ajouter un domaine. Voir *Ajout d'un domaine à la page 2-52* pour obtenir des informations détaillées.
- Supprimer un domaine ou un client. Voir *Suppression d'un domaine ou d'un client à la page 2-53* pour obtenir des informations détaillées.
- Renommer un domaine. Voir *Attribution d'un nouveau nom à un domaine à la page 2-54* pour obtenir des informations détaillées.
- Déplacer un client vers un autre domaine ou serveur OfficeScan. Voir *Déplacement d'un client OfficeScan vers un autre domaine ou un serveur OfficeScan à la page 2-54* pour obtenir des informations détaillées.

Regroupement automatique de clients :

- Trier les clients. Voir *Tri des clients à la page 2-55* pour obtenir des informations détaillées.
- Supprimer un domaine ou client. Voir *Suppression d'un domaine ou d'un client à la page 2-53* pour obtenir des informations détaillées.

Ajout d'un domaine

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Cliquez sur **Gérer l'arborescence des clients** > **Ajouter un domaine**.
3. Saisissez un nom pour le domaine que vous souhaitez ajouter.
4. Cliquez sur **Ajouter**.

Le nouveau domaine apparaît dans l'arborescence des clients.

5. (Facultatif) Créez des sous-domaines.

   a. Sélectionnez le domaine parent.

   b. Cliquez sur **Gérer l'arborescence des clients** > **Ajouter un domaine**.

   c. Saisissez le nom de sous-domaine.

Suppression d'un domaine ou d'un client

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence client, sélectionnez :
   - Un ou plusieurs domaines
   - Un, plusieurs ou tous les clients appartenant à un domaine
3. Cliquez sur **Gérer l'arborescence des clients** > **Supprimer un domaine/client**.
4. Pour supprimer un domaine vide, cliquez sur **Supprimer un domaine/client**. Si le domaine possède des clients et que vous cliquez sur **Supprimer un domaine/client**, le serveur OfficeScan créera de nouveau le domaine et regroupera tous les clients sous ce domaine la prochaine fois que les clients se connectent au serveur OfficeScan. Avant de supprimer le domaine, procédez comme suit :

   a. Déplacez les clients vers d'autres domaines. Pour déplacer les clients vers d'autres domaines, faites-les glisser vers les domaines de destination.

   b. Supprimez tous les clients.

5. Pour supprimer un client, cliquez sur **Supprimer domaine/client**.

Remarque

La suppression d'un client de l'arborescence client ne supprime pas le client OfficeScan de l'ordinateur client. Le client OfficeScan peut toujours effectuer des tâches indépendantes du serveur, telles que la mise à jour des composants. Le serveur n'est cependant pas informé de la présence du client et ne peut donc pas lui envoyer de notifications ou déployer des configurations.

Attribution d'un nouveau nom à un domaine

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Sélectionnez un domaine dans l'arborescence client.
3. Cliquez sur **Gérer l'arborescence des clients** > **Renommer domaine**.
4. Entrez un nouveau nom pour le domaine.
5. Cliquez sur **Renommer**.

   Le nouveau nom de domaine apparaît dans l'arborescence client.

Déplacement d'un client OfficeScan vers un autre domaine ou un serveur OfficeScan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence client, ouvrez un domaine, puis sélectionnez un, plusieurs ou tous les clients.
3. Cliquez sur **Gérer l'arborescence des clients** > **Déplacer client**.
4. Pour déplacer des clients vers un autre domaine :
   - Sélectionnez **Déplacer le ou les clients sélectionnés vers un autre domaine**.

- Sélectionnez le domaine.
- (Facultatif) Appliquez au client les paramètres du nouveau domaine.

Conseil

Vous pouvez également utiliser la fonction glisser-déposer pour déplacer les clients vers un autre domaine dans l'arborescence client.

5. Pour déplacer des clients vers un autre serveur OfficeScan :
   - Sélectionnez **Déplacer le ou les clients sélectionnés vers un autre serveur OfficeScan**.
   - Saisissez le nom ou l'adresse IPv4/IPv6 et le numéro de port HTTP du serveur.
6. Cliquez sur **Déplacer**.

Tri des clients

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence client, exécutez l'une des opérations suivantes :
   - Pour trier tous les clients, cliquez sur l'icône du domaine racine OfficeScan ( ).
   - Pour trier uniquement les clients appartenant à des domaines particuliers, sélectionnez les domaines.
   - Pour trier plusieurs clients ou tous les clients d'un domaine particulier, ouvrez le domaine, puis sélectionnez les clients.
3. Cliquez sur **Gérer l'arborescence des clients** > **Trier les clients**.
4. Cliquez sur **Start**.

5. Cliquez sur **Fermer** lorsque le tri est terminé. Les clients triés devraient désormais appartenir à leurs domaines indiqués.

Chapitre 3

Utilisation de Trend Micro Smart Protection

Ce chapitre présente les solutions Trend Micro™ Smart Protection et explique comment configurer l'environnement requis pour les utiliser.

- *À propos de Trend Micro Smart Protection à la page 3-2*
- *Services Smart Protection à la page 3-3*
- *Sources Smart Protection à la page 3-6*
- *Fichiers de signatures Smart Protection à la page 3-8*
- *Configuration des services Smart Protection à la page 3-13*
- *Utilisation des services Smart Protection à la page 3-31*

À propos de Trend Micro Smart Protection

Trend Micro™ Smart Protection constitue une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques de sécurité et les menaces Internet. Elle repose sur des solutions à la fois locales et hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage, à l'aide de clients légers permettant d'accéder à une combinaison unique de technologies en ligne de messagerie, de file reputation et de sites Web, alliées à des bases de données de menaces. La protection des clients est automatiquement mise à jour et renforcée au fur et à mesure que le nombre de produits, services et utilisateurs accédant au réseau augmente et constitue ainsi un service de protection de voisinage en temps réel pour ses utilisateurs.

Grâce à l'intégration de technologies en ligne de réputation, de scan et de corrélation, les solutions Smart Protection de Trend Micro réduisent la dépendance vis-à-vis des téléchargements de fichiers de signatures traditionnels et éliminent les temps d'attentes habituels liés aux mises à jour de postes de travail.

Le besoin d'une nouvelle solution

Dans l'approche actuelle de la gestion des menaces basées sur les fichiers, les signatures (ou les définitions) requises pour protéger un client sont, pour la plupart, fournies sur la base d'une planification. Trend Micro envoie les signatures par lots vers les clients. À la réception d'une nouvelle mise à jour, le logiciel de protection contre les virus/programme malveillants du client recharge en mémoire ce lot de définitions de signatures de nouveaux risques. En cas de nouveau virus/programme malveillant, cette signature doit à nouveau être mise à jour partiellement ou entièrement et rechargée sur le client pour assurer une protection continue.

Avec le temps, le volume des nouvelles menaces a connu une augmentation significative. Une progression du nombre de menaces quasi-exponentielle est prévue dans les années à venir. Avec un tel taux de croissance, le nombre de risques de sécurité actuellement connus sera prochainement largement dépassé. À l'avenir, le volume des risques de sécurité représentera en soi un nouveau type de risque de sécurité. Il peut avoir un impact sur les performances des serveurs et des postes de travail, l'utilisation de la bande passante du réseau et, en général, le temps nécessaire pour fournir une protection efficace (« délai de protection »).

Trend Micro a adopté une nouvelle approche dans la gestion du volume des menaces. Elle vise à protéger les utilisateurs de Trend Micro contre le risque que représente ce volume lui-même. Cet effort d'innovation tire parti d'une technologie et d'une architecture qui permettent de transférer en ligne le stockage des signatures de virus/programmes malveillants. Trend Micro est ainsi à même de mieux protéger les clients contre le volume de nouveaux risques de sécurité.

Services Smart Protection

Smart Protection comprend des services qui fournissent des bases de données de signatures anti-programmes malveillants, de réputation de sites web et de menaces stockées en ligne.

Les services Smart protection comprennent :

- **Services de File Reputation** : Les services de File Reputation transfèrent un nombre important de signatures anti-programmes malveillants auparavant stockées sur des ordinateurs clients vers des sources Smart Protection. Pour obtenir des informations détaillées, voir *Services de File Reputation à la page 3-3*.
- **Services de réputation de sites Web** : Les services de réputation de sites Web permettent à des sources Smart Protection locales d'héberger des données de réputation d'URL auparavant hébergées uniquement par Trend Micro. Ces deux technologies consomment moins de bande passante lors de la mise à jour des signatures ou de la vérification de la validité des URL. Pour obtenir des informations détaillées, voir *Services de réputation de sites Web à la page 3-4*.
- **Smart Feedback** : Trend Micro continue à collecter les informations envoyées anonymement du monde entier à partir de produits Trend Micro, de façon à identifier proactivement chaque nouvelle menace. Pour obtenir des informations détaillées, voir *Smart Feedback à la page 3-5*.

Services de File Reputation

Les services de File Reputation vérifient la réputation de chaque fichier par rapport à une base de données en ligne étendue. Les informations sur les programmes malveillants étant stockées en ligne, elles sont instantanément accessibles à tous les utilisateurs. Des

réseaux de transmission de contenu et des serveurs de cache très performants garantissent un temps de latence minimum pendant le processus de vérification. L'architecture de client en ligne procure une protection immédiate et élimine la contrainte liée au déploiement de fichiers de signature tout en réduisant sensiblement l'encombrement sur le client.

Les clients doivent être en mode Smart Scan pour pouvoir utiliser les services de File Reputation. Ces clients sont appelés **clients Smart Scan** dans le présent document. Les clients qui ne se trouvent pas en mode Smart Scan et qui n'ont pas recours aux services de File Reputation sont appelés **clients de scan traditionnel**. Les administrateurs OfficeScan peuvent configurer plusieurs ou tous les clients pour qu'ils soient en mode Smart Scan.

Services de réputation de sites Web

Dotée de l'une des plus grandes bases de données de réputation de domaine du monde, la technologie de réputation de sites Web de Trend Micro assure le suivi de la crédibilité des domaines Web en attribuant un score de réputation dépendant de facteurs tels que l'ancienneté du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. La réputation des sites Web continue ensuite à analyser les sites et à bloquer les utilisateurs tentant d'accéder à ceux qui sont infectés. Les fonctionnalités de réputation de sites Web permettent de garantir que les pages consultées par les utilisateurs sont sûres et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing visant à duper les utilisateurs afin de leur faire divulguer des informations personnelles. Pour une plus grande précision et une réduction des faux positifs, la technologie de réputation de sites Web de Trend Micro affecte des scores de réputation à des pages et liens spécifiques de chaque site, plutôt que de classer comme suspects des sites entiers ou de les bloquer. En effet, il arrive souvent que seule une portion d'un site légitime ait été piratée et les réputations peuvent changer de manière dynamique au fil du temps

Les clients OfficeScan sujets aux stratégies de réputation de sites Web utilisent les services de réputation de sites Web. Les administrateurs OfficeScan peuvent soumettre tous les clients ou certains d'entre eux aux stratégies de réputation de sites Web.

Smart Feedback

Trend Micro Smart Feedback assure la communication permanente entre les produits Trend Micro et les centres et technologies de recherche des menaces de la société, opérationnels 24h/24h et 7 jours/7. Chaque nouvelle menace identifiée par un contrôle de réputation de routine d'un seul client met automatiquement à jour toutes les bases de données de menaces de Trend Micro, et empêche que cette menace ne survienne à nouveau chez un autre client.

Grâce à l'analyse constante des données de menaces collectées par son vaste réseau mondial de clients et de partenaires, Trend Micro assure une protection automatique et en temps réel contre les dernières menaces, offrant ainsi une sécurité « unifiée », très semblable à une surveillance de voisinage automatisée qui implique la communauté dans la protection de chacun. La confidentialité des informations personnelles ou professionnelles d'un client est toujours protégée car les données sur les menaces qui sont collectées reposent sur la réputation de la source de communication et non sur le contenu de la communication en question.

Exemples d'informations envoyées à Trend Micro :

- les sommes de contrôles des fichiers
- les sites Web visités
- les données relatives aux fichiers, y compris, leur taille et l'adresse de leur emplacement
- les noms des fichiers exécutables

Vous pouvez interrompre à tout moment votre participation au programme depuis la console Web.

Conseil

Il n'est pas obligatoire de participer à Smart Feedback pour protéger ses ordinateurs. La participation de l'utilisateur est optionnelle et il peut y mettre fin à tout moment. Trend Micro recommande aux utilisateurs de participer à Smart Feedback afin d'assurer une meilleure protection globale à tous les clients Trend Micro.

Pour davantage d'informations à propos de Smart Protection Network, consultez :

http://fr.trendmicro.com/fr/technology/smart-protection-network

Sources Smart Protection

Trend Micro fournit des services de File Reputation et de sites Web à OfficeScan et aux sources Smart Protection.

Les sources Smart Protection hébergent la majorité des définitions de signatures de virus/programmes malveillants dans le cadre des services de File Reputation. Les clients OfficeScan hébergent les définitions restantes. Un client envoie des requêtes de scan aux sources Smart Protection si ses propres définitions de signature ne parviennent pas à déterminer la menace que présente un fichier. Les sources Smart Protection déterminent cette menace à l'aide des informations d'identification.

Les sources Smart Protection hébergent des données de réputation de sites Web disponibles uniquement via les serveurs hébergés Trend Micro dans le cadre de la fourniture des services de réputation de sites Web. Un client envoie des requêtes de réputation de sites Web aux sources Smart Protection pour vérifier la réputation des sites Web auxquels un utilisateur tente d'accéder. Le client compare la réputation d'un site Web à la stratégie appliquée en la matière sur l'ordinateur pour déterminer si l'accès au site est approuvé ou bloqué.

La source Smart Protection Server à laquelle un client se connecte dépend de l'emplacement de l'ordinateur client. Les clients peuvent se connecter à Trend Micro Smart Protection Network ou à un serveur Smart Protection Server.

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ est une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques liés à la sécurité et les menaces Internet. Il repose sur des solutions à la fois sur site et Trend Micro hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage. Smart Protection Network utilise des clients légers pour accéder à un ensemble unique de technologies en ligne de corrélation d'e-mail, de réputation de fichiers de sites Web et de bases de données de menaces. À mesure que de nouveaux produits, services et utilisateurs accèdent au réseau, la sécurité des clients est

automatiquement mise à jour et renforcée, créant ainsi un service de protection de voisinage en temps réel pour les utilisateurs.

Pour davantage d'informations à propos de Smart Protection Network, consultez :

www.smartprotectionnetwork.com

Smart Protection Server

Les serveurs Smart Protection Server sont mis à la disposition des utilisateurs qui ont accès à leur réseau d'entreprise local. Les serveurs locaux localisent les services Smart Protection sur le réseau d'entreprise afin d'assurer une efficacité optimale.

Il existe deux types de serveurs Smart Protection Server :

- **Smart Protection Server intégré** : Le programme OfficeScan Setup comprend un serveur Smart Protection Server intégré qui s'installe sur le même ordinateur que le serveur OfficeScan. Après l'installation, vous pouvez gérer les paramètres de ce serveur intégré à partir de la console Web d'OfficeScan. Le serveur intégré est conçu pour les déploiements de petite envergure d'OfficeScan, pour lesquels le nombre de clients est au maximum de 1 000. Pour les déploiements de plus grande envergure, le serveur Smart Protection Server autonome est requis.
- **Serveur Smart Protection Server autonome** : Un serveur Smart Protection Server autonome s'installe sur un serveur VMware ou Hyper-V. Le serveur autonome possède une console d'administration séparée et n'est pas géré depuis la console Web d'OfficeScan.

Sources Smart Protection comparées

Le tableau suivant met en évidence les différences entre Smart Protection Network et Smart Protection Server.

TABLEAU 3-1. Sources Smart Protection comparées

BASE DE COMPARAISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Disponibilité	Disponible pour les clients internes, c'est-à-dire ceux qui répondent aux critères d'emplacement spécifiés sur la console Web d'OfficeScan	Disponible principalement pour les clients externes, c'est-à-dire ceux qui ne répondent pas aux critères d'emplacement spécifiés sur OfficeScan web console
Objet	Conçu dans le but de localiser les services Smart Protection sur le réseau d'entreprise afin d'assurer une efficacité optimale	Infrastructure Internet d'envergure mondiale visant à fournir des services Smart Protection aux clients qui ne bénéficient pas d'un accès direct à leur réseau d'entreprise
Administration	Les administrateurs OfficeScan installent et gèrent ces sources Smart Protection.	Trend Micro gère cette source.
Source de mise à jour des signatures	Trend Micro ActiveUpdate Server	Trend Micro ActiveUpdate Server
Protocoles de connexion client	HTTP et HTTPS	HTTPS

Fichiers de signatures Smart Protection

Les fichiers de signatures Smart Protection sont utilisés dans le cadre des services de File Reputation et de sites Web. Ils sont publiés par Trend Micro par l'intermédiaire du serveur Trend Micro ActiveUpdate.

Smart Scan Agent Pattern

Le fichier Smart Scan Agent Pattern est mis à jour quotidiennement. Il se télécharge depuis la source de mise à jour des clients OfficeScan (c.-à-d. le serveur OfficeScan ou une source de mise à jour personnalisée); La source de mise à jour déploie par la suite le fichier de signatures sur les clients Smart Scan.

Remarque

Les clients Smart Scan sont des clients OfficeScan que les administrateurs ont configuré de façon à ce qu'ils utilisent les services de File Reputation. Les clients n'ayant pas recours aux services de File Reputation sont désignés par clients scan traditionnel.

Les clients Smart Scan utilisent le fichier Smart Scan Agent Pattern lors d'un scan ayant pour but de détecter les risques de sécurité. Si le fichier de signatures ne peut déterminer les risques impliqués par un fichier, un autre fichier de signatures, appelé Smart Scan Pattern, est appliqué.

Smart Scan Pattern

Le fichier Smart Scan Pattern est mis à jour toutes les heures. Il se télécharge à partir de sources Smart Protection. Les clients Smart Scan ne téléchargent pas le fichier Smart Scan Pattern. Les clients vérifient les menaces potentielles par rapport au fichier Smart Scan Pattern en envoyant des requêtes de scan aux sources Smart Protection.

Liste de blocage de sites Web

Les sources Smart Protection téléchargent la liste de blocage des sites. Les clients OfficeScan qui sont soumis aux stratégies de réputation de sites Web ne téléchargent pas la liste de blocage de sites Web.

Remarque

Les administrateurs peuvent soumettre tous les clients ou certains d'entre eux aux stratégies de réputation de sites Web.

Les clients soumis aux stratégies de réputation de sites Web vérifient la réputation d'un site par rapport à la liste de blocage de sites Web. Pour cela, ils envoient une requête de réputation de site Web à une source Smart Protection. Le client compare les données de réputation qu'il reçoit de la source Smart Protection à la stratégie de réputation de sites Web en vigueur sur l'ordinateur. Selon la stratégie appliquée, le client approuve ou bloque l'accès au site.

Processus de mise à jour des signatures Smart Protection

Toutes les mises à jour de fichiers Smart Protection Pattern proviennent du serveur Trend Micro ActiveUpdate Server.

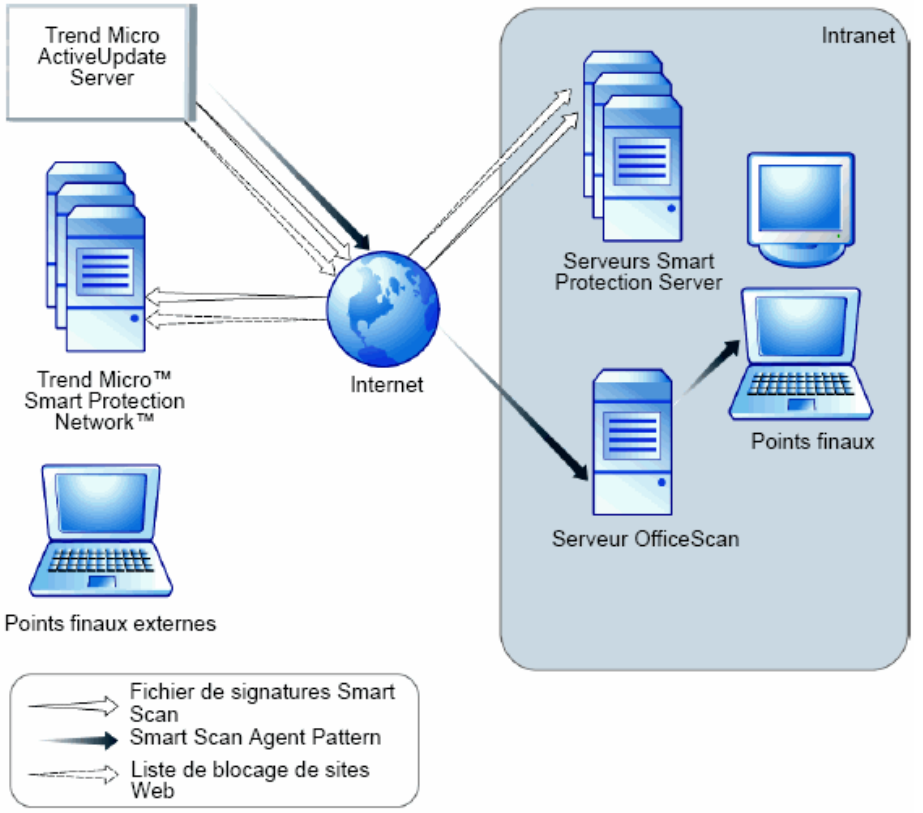


FIGURE 3-1. Processus de mise à jour des signatures

Utilisation des signatures Smart Protection

Un client OfficeScan utilise le fichier Smart Scan Agent Pattern pour procéder à un scan des risques de sécurité. Il interroge uniquement le fichier Smart Scan Pattern dans le cas où le fichier Smart Scan Agent Pattern ne parvient pas à déterminer si un fichier présente une menace ou non. Lorsqu'un utilisateur tente d'accéder à un site Web, le client interroge la liste de blocage des sites Web. La technologie de filtrage avancée permet au client de « mettre en mémoire cache » les résultats de la requête. Ainsi, il n'est plus nécessaire d'envoyer plusieurs fois une seule et même question.

Les clients actuellement présents dans votre intranet peuvent se connecter à un serveur Smart Protection Server pour interroger le fichier Smart Scan Pattern ou la liste de blocage des sites Web. Une connexion réseau est requise pour se connecter au serveur Smart Protection Server. Si plusieurs serveurs Smart Protection Server ont été configurés, les administrateurs peuvent déterminer la priorité de connexion.

Conseil

Installez plusieurs serveurs Smart Protection Server pour assurer la continuité de la protection dans le cas où la connexion à un serveur Smart Protection Server n'est pas possible.

Les clients qui ne se trouvent pas dans votre intranet peuvent se connecter à Trend Micro Smart Protection Network pour envoyer des requêtes. Une connexion Internet est requise pour se connecter à Smart Protection Network.

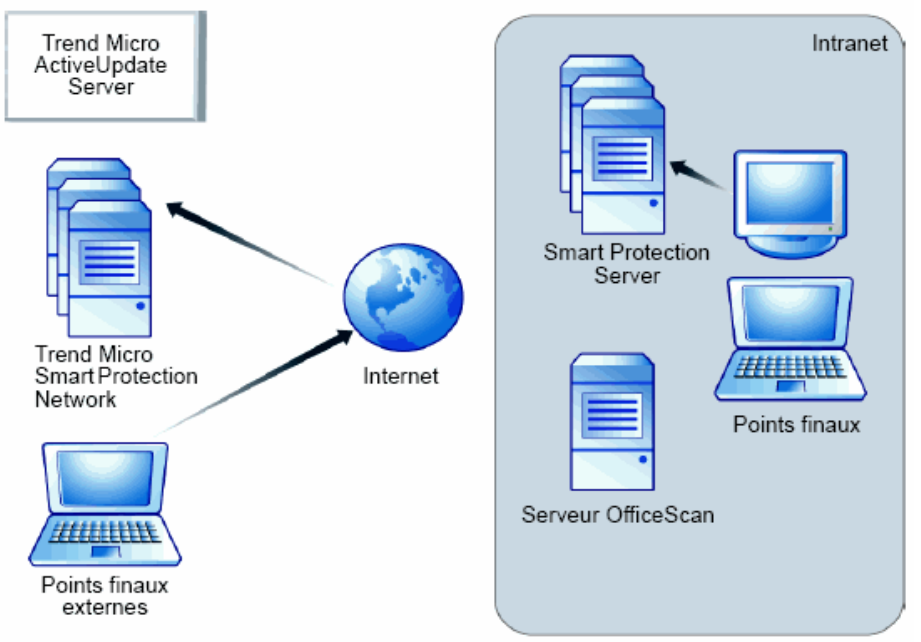


FIGURE 3-2. Processus de requête

Les clients n'ayant pas accès au réseau ou à Internet bénéficient toujours de la protection fournie par le fichier Smart Scan Agent Pattern et par le cache contenant les résultats de requêtes précédentes. La protection est réduite uniquement lorsqu'une nouvelle requête s'avère nécessaire et que le client ne parvient pas à atteindre une source Smart Protection après plusieurs tentatives. Dans ce cas, un client marque le fichier pour vérification et autorise temporairement l'accès au fichier. Lorsque la connexion à une source Smart Protection est restaurée, tous les fichiers marqués d'un indicateur sont scannés à nouveau. L'action de scan appropriée est ensuite effectuée sur les fichiers dont la menace a été confirmée.

Le tableau suivant récapitule la portée de la protection en fonction de l'emplacement du client.

TABLEAU 3-2. Comportements de protection en fonction de l'emplacement

EMPLACEMENT	FICHIER DE SIGNATURES ET COMPORTEMENT DE REQUÊTE
Accès à l'intranet	• **Fichier de signatures** : les clients téléchargent le fichier Smart Scan Agent Pattern depuis le serveur OfficeScan ou depuis une source de mise à jour personnalisée. • **Requêtes de File Reputation et de réputation de sites Web** : Les clients se connectent au Smart Protection Server pour les requêtes.
Sans accès à l'intranet mais avec une connexion à Smart Protection Network	• **Fichier de signatures** : les clients ne téléchargent le dernier fichier Smart Scan Agent Pattern que si une connexion à un serveur OfficeScan ou à une source de mise à jour personnalisée est disponible. • **Requêtes de File Reputation et de réputation de sites Web** : les clients se connectent au serveur Smart Protection Network pour les requêtes.
Sans accès à l'intranet et sans connexion à Smart Protection Network	• **Fichier de signatures** : les clients ne téléchargent le dernier fichier Smart Scan Agent Pattern que si une connexion à un serveur OfficeScan ou à une source de mise à jour personnalisée est disponible. • **Requêtes de File Reputation et de réputation de sites Web** : les clients ne reçoivent pas de résultats de requête et dépendent du Smart Scan Agent Pattern ainsi que du cache contenant les résultats de requêtes précédentes.

Configuration des services Smart Protection

Avant que les clients puissent utiliser les services de File Reputation et de sites Web, assurez-vous que l'environnement Smart Protection a correctement été configuré. Vérifiez ce qui suit :

- *Installation du serveur Smart Protection Server à la page 3-14*

- *Gestion du serveur Smart Protection Server intégré à la page 3-19*
- *Liste des sources Smart Protection à la page 3-23*
- *Paramètres du proxy de la connexion du client à la page 3-30*
- *Installations de Trend Micro Network VirusWall à la page 3-31*

Installation du serveur Smart Protection Server

Vous pouvez utiliser le serveur Smart Protection Server intégré ou autonome si le nombre de clients est inférieur à 1 000. S'il y a plus de 1 000 clients, installez un serveur Smart Protection Server autonome.

Trend Micro recommande que vous installiez plusieurs serveurs Smart Protection Server à des fins de basculement. Les clients ne pouvant pas se connecter à un serveur particulier tenteront de se connecter aux autres serveurs que vous aurez configurés.

Du fait que le serveur intégré et le serveur OfficeScan s'exécutent sur le même ordinateur, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Envisagez d'utiliser un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours.

Installation du serveur Smart Protection Server autonome

Pour obtenir des instructions sur l'installation et la gestion du serveur Smart Protection Server autonome, consultez le *Manuel d'installation et e mise à jour Trend Micro Smart Protection Server*.

Installation du serveur Smart Protection Server intégré

Si vous avez installé le serveur intégré pendant l'installation du serveur OfficeScan :

- Activez le serveur intégré et configurez les paramètres du serveur. Pour obtenir des informations détaillées, voir *Gestion du serveur Smart Protection Server intégré à la page 3-19*.
- Si le serveur intégré et le client OfficeScan coexistent sur le même ordinateur serveur, envisagez la désactivation du pare-feu OfficeScan. Le pare-feu OfficeScan

est conçu pour être utilisé par les ordinateurs clients; il peut affecter les performances s'il est activé sur les ordinateurs serveurs. Pour obtenir des instructions sur la désactivation du pare-feu, voir *Activation ou désactivation du pare-feu OfficeScan à la page 11-6*.

Remarque

Examinez les conséquences de la désactivation du pare-feu et assurez-vous qu'elle est conforme à vos plans en matière de sécurité.

Conseil

Installez Smart Protection Server intégré à la fin de l'installation d'OfficeScan en utilisant l'*Outil du serveur Smart Protection Server intégré à la page 3-15*.

Outil du serveur Smart Protection Server intégré

L'outil Smart Protection intégré d'OfficeScan de Trend Micro permet aux administrateurs d'installer ou de désinstaller un serveur Smart Protection Server intégré une fois que l'installation du serveur OfficeScan est terminée. La version actuelle d'OfficeScan ne permet pas aux administrateurs d'installer/de supprimer un serveur Smart Protection Server intégré, une fois que l'installation du serveur OfficeScan est terminée. Cet outil améliore la flexibilité des fonctionnalités d'installation par rapport aux versions précédentes d'OfficeScan.

Avant d'effectuer l'installation du serveur Smart Protection Server intégré, vous devez importer les paramètres suivants sur votre serveur SP1 OfficeScan 10.6 mis à niveau :

- Structures de domaine
- Les paramètres au niveau de la racine et du domaine :
  - Configurations de scan pour tous les types de scan (scan en temps réel, manuel, programmé et immédiat)
  - Configurations de la réputation de sites Web
  - Liste d'URL approuvés
  - Paramètres de surveillance des comportements

  - Paramètres de contrôle des dispositifs
  - Paramètres de prévention contre la perte de données
  - Privilèges et autres paramètres
  - Paramètres des services complémentaires
  - Liste des spywares/graywares approuvés
- Paramètres clients généraux
- Emplacement de l'ordinateur
- Stratégies et profils de pare-feu
- Sources Smart Protection
- Programme de mise à jour du serveur
- Source et programme de mise à jour du client
- Notifications
- Paramètres proxy

Tâche

1. Ouvrez une fenêtre d'invite et accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\ISPSInstaller` dans lequel se trouve le fichier `ISPSInstaller.exe`.
2. Exécutez `ISSSInstaller.exe` en utilisant l'une des commandes suivantes :

TABLEAU 3-3. Options du programme d'installation.

COMMANDE	DESCRIPTION
`ISPSInstaller.exe /i`	Installe le serveur intégré Smart Protection Server en utilisant les paramètres de port par défaut suivants : • Port HTTP file reputation : 1234 • Port HTTPS file reputation : 1234 • Port de réputation de sites Web : 1236
`ISPSInstaller.exe /i /f:[numéro de port] /s:[numéro de port] /w:[numéro de port]`	Installe le serveur intégré Smart Protection Server en utilisant les ports spécifiés, sur lesquels : • `/f:[numéro de port]` représente le port HTTP file reputation • `/s:[numéro de port]` représente le port HTTPS file reputation • `/w:[numéro de port]` représente le port de réputation de sites Web **Remarque** Une valeur par défaut est automatiquement attribuée au port non spécifié.
`ISPSInstaller.exe /u`	Désinstalle le serveur intégré Smart Protection Server

3. Une fois que l'installation est terminée, ouvrez la console Web OfficeScan et vérifiez les informations suivantes :

   - Ouvrez la console d'administration **Microsoft Management Console** (en saisissant `services.msc` dans le menu **Démarrer**) et assurez-vous que Trend Micro Local Web Classification Server et Trend Micro Smart Scan Server indiquent l'état « Démarré » dans la liste.

   - Ouvrez le **Gestionnaire des tâches Windows**. Dans l'onglet **Processus**, vérifiez que `iCRCService.exe` et `LWCSService.exe` sont en cours d'exécution,

- Sur la console Web OfficeScan, vérifiez que l'élément de menu **Smart Protection** > **Serveur intégré** est bien affiché.

Pratiques recommandées relatives au serveur Smart Protection Server

Optimisez les performances des serveurs Smart Protection Server en exécutant les tâches suivantes :

- Évitez d'effectuer un scan manuel et un scan programmé simultanément. Échelonnez les scans par groupes.
- Configurez les clients de manière à éviter qu'ils effectuent un scan immédiat simultanément.
- Personnalisez les serveurs Smart Protection Server pour les connexions réseau lentes (environ 512 Kbits/s) en effectuant les modifications suivantes dans le fichier `ptngrowth.ini`.

Personnalisation du fichier « ptngrowth.ini » pour le serveur autonome

Tâche

1. Ouvrez le fichier `ptngrowth.ini` dans `/var/tmcss/conf/`.
2. Modifiez le fichier `ptngrowth.ini` file en utilisant les valeurs recommandées suivantes :
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Enregistrez le fichier `ptngrowth.ini`.
4. Redémarrez le service `lighttpd` en saisissant la commande suivante dans l'interface de ligne de commande (CLI) :

- `redémarrge du service lighttpd`

Personnalisation du fichier « ptngrowth.ini » pour le serveur intégré

Tâche

1. Ouvrez le fichier `ptngrowth.ini`dans le <*Dossier d'installation du serveur*> `\PCCSRV\WSS\`.
2. Modifiez le fichier `ptngrowth.ini` file en utilisant les valeurs recommandées suivantes :
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Enregistrez le fichier `ptngrowth.ini`.
4. Redémarrez le service `Trend Micro Smart Protection Server`.

Gestion du serveur Smart Protection Server intégré

Gérez le serveur Smart Protection Server intégré à l'aide des tâches suivantes :

- Activation des services de File Reputation et des services de réputation de sites Web du serveur intégré
- enregistrement des adresses du serveur intégré
- mise à jour des composants du serveur intégré
- configuration de la liste des URL approuvées/bloquées du serveur intégré.

Activation des services de File Reputation et des services de réputation de sites Web du serveur intégré

Pour que les clients puissent envoyer des requêtes de scan et de réputation de sites Web au serveur intégré, les services de File Reputation et les services de réputation de sites

Web doivent être activés. L'activation de ces services permet également au serveur intégré de mettre à jour les composants à partir du serveur ActiveUpdate.

Ces services sont automatiquement activés si vous avez choisi d'installer le serveur intégré pendant l'installation du serveur OfficeScan Server.

Si vous désactivez ces services, assurez-vous d'avoir installé les serveurs autonomes Smart Protection Server vers lesquels les clients envoient des requêtes.

Enregistrement des adresses du serveur intégré

Pour configurer la liste des sources Smart Protection pour les clients internes, vous aurez besoin des adresses du serveur intégré. Pour plus de détails sur la liste, voir *Liste des sources Smart Protection à la page 3-23*.

Lorsque les clients envoient des requêtes de scans au serveur intégré, ils identifient le serveur par l'une des deux adresses des services de File Reputation : l'adresse HTTP ou l'adresse HTTPS. Une connexion avec l'adresse HTTPS est plus sécurisée, tandis qu'une connexion avec l'adresse HTTP utilise moins de bande passante.

Lorsque les clients envoient des requêtes de réputation de sites Web, ils identifient le serveur intégré par son adresse de services de réputation de sites Web.

Conseil

Les clients gérés par un autre serveur OfficeScan peuvent également se connecter à ce serveur intégré. Sur l'autre console Web du serveur OfficeScan, ajoutez l'adresse du serveur intégré à la liste des sources Smart Protection.

Mise à jour des composants du serveur intégré

Le serveur intégré met à jour les composants suivants :

- **Smart Scan Pattern** : Les clients vérifient les menaces potentielles par rapport au fichier Smart Scan Pattern en envoyant des requêtes de scan au serveur intégré.
- **Liste de blocage de sites Web** : les clients soumis aux stratégies de réputation des sites Web vérifient la réputation d'un site par rapport à la Liste de blocage de sites Web. Pour cela, ils envoient une requête de réputation au serveur intégré.

Mettez manuellement à jour ces composants ou configurez un programme de mise à jour. Le serveur intégré télécharge les composants depuis le serveur ActiveUpdate.

Remarque

Un serveur intégré IPv6 pur ne peut pas directement faire une mise à jour à partir du serveur Trend Micro ActiveUpdate Server. Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur intégré de se connecter au serveur ActiveUpdate.

Configuration de la liste des URL approuvées/bloquées du serveur intégré

Les clients disposent de leur propre liste des URL approuvées/bloquées. Configurez la liste des clients lorsque vous mettez en place des stratégies de réputation de sites Web (voir *Stratégies de réputation de sites Web à la page 10-3* pour plus d'informations). Toute URL figurant dans la liste d'un client est automatiquement approuvée ou bloquée.

Le serveur intégré dispose de sa propre liste d'URL approuvées ou bloquées. Si une URL ne figure pas dans la liste d'un client, celui-ci envoie une requête de réputation de sites Web au serveur intégré (si le serveur intégré a été attribué comme source Smart Protection). Si l'URL figure dans la liste des URL approuvées/bloquées du serveur intégré, celui-ci indique au client s'il doit approuver ou bloquer l'URL.

Remarque

La liste des URL bloquées a une priorité plus élevée que la liste de blocage de sites Web.

Pour ajouter des URL à la liste des URL approuvées/bloquées du serveur intégré, importez une liste depuis un serveur Smart Protection Server autonome. Vous ne pouvez pas ajouter d'URL manuellement.

Configuration des paramètres du serveur Smart Protection Server intégré

Tâche

1. Accédez à **Smart Protection** > **Serveur intégré**.

2. Sélectionnez **Activer les services de File Reputation**.
3. Sélectionnez le protocole (HTTP ou HTTPS) que les clients utiliseront pour envoyer des requêtes de scan au serveur intégré.
4. Sélectionnez **Activer les services de réputation de sites Web**.
5. Enregistrez les adresses du serveur intégré dans la colonne Adresse du serveur.
6. Pour mettre à jour les composants du serveur intégré :
   - Consultez les versions actuelles du fichier Smart Scan Pattern et de la liste de blocage de sites Web. Si une mise à jour est disponible, cliquez sur **Mettre à jour**. Le résultat de la mise à jour s'affiche dans la partie supérieure de l'écran.
   - Pour mettre automatiquement à jour le fichier de signatures :
     a. Sélectionnez **Activer les mises à jour programmées**.
     b. Indiquez si la mise à jour doit avoir lieu toutes les heures ou toutes les 15 minutes.
     c. Dans **Services de File Reputation**, sélectionnez une source de mise à jour. Le fichier Smart Scan Pattern sera mis à jour à partir de cette source.
     d. Dans **Services de réputation de sites Web**, sélectionnez une source de mise à jour. La liste de blocage de sites Web sera mise à jour à partir de cette source.

Remarque

- Si vous choisissez le serveur ActiveUpdate comme source de mise à jour, assurez-vous qu'il dispose d'une connexion Internet et, si vous utilisez un serveur proxy, testez la connexion Internet pour voir si elle peut être établie en utilisant les paramètres du proxy. Voir *Proxy pour les mises à jour du serveur OfficeScan à la page 5-18* pour obtenir des informations détaillées.
- Si vous choisissez une source de mise à jour personnalisée, définissez l'environnement approprié et mettez à jour les ressources de cette source de mise à jour. Assurez-vous également qu'il existe une connexion opérationnelle entre le serveur et cette source de mise à jour. Si vous avez besoin d'aide pour définir une source de mise à jour, contactez votre service d'assistance.

7. Pour configurer la liste des URL approuvées/bloquées du serveur intégré :

   a. Cliquez sur **Importer** pour renseigner la liste à l'aide d'URL venant d'un fichier .csv pré-formaté. Vous pouvez obtenir le fichier `.csv` à partir d'un serveur Smart Protection Server autonome.

   b. Si vous disposez d'une liste existante, cliquez sur **Exporter** pour enregistrer la liste dans un fichier `.csv`.

8. Cliquez sur **Enregistrer**.

Liste des sources Smart Protection

Les clients envoient des requêtes aux sources Smart Protection dans le cadre du scan des risques de sécurité et de la détermination de la réputation d'un site Web.

Prise en charge d'IPv6 pour les sources Smart Protection

Un client IPv6 pur ne peut pas envoyer directement de requêtes à des sources IPv4 pures telles que :

- Smart Protection Server 2.0 (intégré ou autonome)

Remarque

IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5.

- Trend Micro Smart Protection Network

De même, un client IPv4 pur ne peut pas envoyer de requêtes à des serveurs Smart Protection IPv6 purs.

Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients de se connecter aux sources.

Sources Smart Protection et emplacement de l'ordinateur

La source Smart Protection à laquelle le client se connecte dépend de l'emplacement de l'ordinateur client.

Pour obtenir des informations détaillées sur la configuration des paramètres d'emplacement, voir *Emplacement de l'ordinateur à la page 13-2*.

TABLEAU 3-4. Sources Smart Protection par emplacement

EMPLACEMENT	SOURCES SMART PROTECTION
Externe	Les clients externes peuvent envoyer des requêtes de scan et de réputation de sites Web à Trend Micro Smart Protection Network.
Interne	Les clients internes peuvent envoyer des requêtes de scan et de réputation de sites Web aux serveurs Smart Protection Server ou à Trend Micro Smart Protection Network. Si vous avez installé des serveurs Smart Protection Server, configurez la liste des sources Smart Protection sur OfficeScan web console. Un client interne sélectionne un serveur de la liste lorsqu'il doit émettre une requête. S'il ne parvient pas à se connecter au premier serveur, il en sélectionne un autre dans la liste. **Conseil** Affectez un serveur Smart Protection Server autonome comme source de scan principale et le serveur intégré comme source de secours. Cela réduit le trafic de requêtes adressées à l'ordinateur qui héberge le serveur OfficeScan et le serveur intégré. Le serveur autonome peut également traiter plus de requêtes. Vous pouvez configurer une liste standard ou personnalisée de sources Smart Protection. La liste standard est utilisée par tous les clients internes. Une liste personnalisée définit une plage d'adresses IP. Si l'adresse IP d'un client interne figure dans cette plage, le client utilise la liste personnalisée.

Configuration de la liste standard des sources Smart Protection

Tâche

1. Accédez à **Smart Protection** > **Sources Smart Protection**.
2. Cliquez sur l'onglet **Clients internes**.
3. Sélectionnez **Utiliser la liste standard (qui sera utilisée par tous les clients internes)**.

4. Cliquez sur le lien **Liste standard**.

   Un nouvel écran s'affiche.

5. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

6. Indiquez le nom d'hôte ou l'adresse IPv4/IPv6 du serveur Smart Protection. Si vous spécifiez une adresse IPv6, placez-la entre parenthèses.

   Remarque

   Indiquez le nom d'hôte si des clients IPv4 et IPv6 se connectent au serveur Smart Protection Server.

7. Sélectionnez Services de File Reputation. Les clients envoient leurs requêtes de scan à l'aide du protocole HTTP ou HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

   a. Si vous souhaitez que les clients utilisent le protocole HTTP, entrez le port d'écoute du serveur pour les requêtes HTTP. Si vous souhaitez que les clients utilisent le protocole HTTPS, sélectionnez SSL et entrez le port d'écoute du serveur pour les requêtes HTTPS.

   b. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.

   Conseil

   Les ports d'écoute font partie de l'adresse du serveur. Pour obtenir l'adresse du serveur :

   Pour le serveur intégré, ouvrez la console Web OfficeScan et accédez au **Smart Protection** > **Serveur intégré**.

   Pour le serveur autonome, ouvrez la console du serveur autonome et accédez à l'écran **Résumé**.

8. Sélectionnez **Services de réputation de sites Web**. Les clients envoient leurs requêtes de réputation de sites Web à l'aide du protocole HTTP. Le protocole HTTPS n'est pas pris en charge.

a. Entrez le port d'écoute du serveur pour les requêtes HTTP.

b. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.

9. Cliquez sur **Enregistrer**.

L'écran se ferme.

10. Répétez les étapes précédentes pour ajouter d'autres serveurs.

11. En haut de l'écran, sélectionnez **Ordre** ou **Aléatoire**.

- **Ordre** : les clients sélectionnent les serveurs dans l'ordre selon lequel ils apparaissent dans la liste. Si vous sélectionnez **Ordre**, utilisez les flèches sous la colonne **Ordre** pour déplacer les serveurs vers le haut ou le bas de la liste.
- **Aléatoire** : les clients sélectionnent des serveurs de façon aléatoire.

Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même ordinateur, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours.

---

12. Exécutez des tâches diverses présentées à l'écran.

- Si vous avez exporté une liste à partir d'un autre serveur et souhaitez l'importer dans cet écran, cliquez sur **Importer** et localisez le fichier `.dat`. La liste est chargée à l'écran.
- Pour exporter la liste dans un fichier `.dat`, cliquez sur **Exporter**, puis sur **Enregistrer**.
- Pour actualiser l'état de service des serveurs, cliquez sur **Actualiser**.
- Cliquez sur le nom du serveur pour effectuer l'une des opérations suivantes :
  - Afficher ou modifier les informations sur le serveur.

- Afficher l'adresse complète du serveur pour les services de réputation de sites Web ou de fichiers.

- Pour ouvrir la console pour un serveur Smart Protection Server, cliquez sur **Lancer la console**.

  - Pour le serveur Smart Protection Server intégré, l'écran de configuration du serveur s'affiche.

  - Pour les serveurs Smart Protection Server autonomes et le serveur Smart Protection Server intégré d'un autre serveur OfficeScan, l'écran de connexion à la console s'affiche.

- Pour supprimer une entrée, activez la case à cocher du serveur, puis cliquez sur **Supprimer**.

13. Cliquez sur **Enregistrer**.

    L'écran se ferme.

14. Cliquez sur **Notifier tous les clients**.

Configuration des listes personnalisées des sources Smart Protection

Tâche

1. Accédez à **Smart Protection** > **Sources Smart Protection**.

2. Cliquez sur l'onglet **Clients internes**.

3. Sélectionnez **Utilisez les listes personnalisées basées sur les adresses IP des clients**.

4. (Facultatif) Sélectionnez U**tilisez la liste standard lorsqu'aucun serveur des listes personnalisées n'est disponible**.

5. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

6. Dans la section **Plage IP**, spécifiez une plage d'adresses IPv4 ou IPv6, ou les deux.

Remarque

Les clients ayant une adresse IPv4 peuvent se connecter à des serveurs Serveurs Smart Protection Server IPv4 pur ou double pile. Les clients ayant une adresse IPv6 peuvent se connecter à des serveurs Serveurs Smart Protection Server IPv6 ou double pile. Les clients ayant aussi bien une adresse IPv4 qu'une adresse IPv6, s'enregistrent sur n'importe quel serveur Smart Protection Server.

7. Dans la section **Paramètres proxy**, indiquez les paramètres proxy que les clients utiliseront pour se connecter aux serveurs Smart Protection Server.

   a. Sélectionnez **Utiliser un serveur proxy pour la communication entre le client et Smart Protection Server**.

   b. Indiquez le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.

   c. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

8. Dans la **Liste des serveurs Smart Protection Server personnalisée**, ajoutez les serveurs Smart Protection Server.

   a. Indiquez le nom d'hôte ou l'adresse IPv4/IPv6 du serveur Smart Protection. Si vous spécifiez une adresse IPv6, placez-la entre parenthèses.

      Remarque

      Indiquez le nom d'hôte si des clients IPv4 et IPv6 se connectent au serveur Smart Protection Server.

   b. Sélectionnez **Services de File Reputation**. Les clients envoient leurs requêtes de scan à l'aide du protocole HTTP ou HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

      i. Si vous souhaitez que les clients utilisent le protocole HTTP, entrez le port d'écoute du serveur pour les requêtes HTTP. Si vous souhaitez que les clients utilisent le protocole HTTPS, sélectionnez **SSL** et entrez le port d'écoute du serveur pour les requêtes HTTPS.

      ii. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.

Conseil

Les ports d'écoute font partie de l'adresse du serveur. Pour obtenir l'adresse du serveur :

Pour le serveur intégré, ouvrez la console Web OfficeScan et accédez au **Smart Protection** > **Serveur intégré**.

Pour le serveur autonome, ouvrez la console du serveur autonome et accédez à l'écran Résumé.

c. Sélectionnez **Services de réputation de sites Web**. Les clients envoient leurs requêtes de réputation de sites Web à l'aide du protocole HTTP. Le protocole HTTPS n'est pas pris en charge.

   i. Entrez le port d'écoute du serveur pour les requêtes HTTP.

   ii. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.

d. Cliquez sur **Ajouter à la liste**.

e. Répétez les étapes précédentes pour ajouter d'autres serveurs.

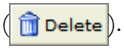
f. Sélectionnez **Ordre** ou **Aléatoire**.

   - **Ordre** : les clients sélectionnent les serveurs dans l'ordre selon lequel ils apparaissent dans la liste. Si vous sélectionnez **Ordre**, utilisez les flèches sous la colonne **Ordre** pour déplacer les serveurs vers le haut ou le bas de la liste.
   - **Aléatoire** : les clients sélectionnent des serveurs de façon aléatoire.

Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même ordinateur, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours.

g. Exécutez des tâches diverses présentées à l'écran.

- Pour actualiser l'état de service des serveurs, cliquez sur **Actualiser**.
- Pour ouvrir la console pour un serveur Smart Protection Server, cliquez sur **Lancer la console**.
  - Pour le serveur Smart Protection Server intégré, l'écran de configuration du serveur s'affiche.
  - Pour les serveurs Smart Protection Server autonomes et le serveur Smart Protection Server intégré d'un autre serveur OfficeScan, l'écran de connexion à la console s'affiche.
- Pour supprimer une entrée, cliquez sur **Supprimer** (

).

9. Cliquez sur **Enregistrer**.

   L'écran se ferme. La liste que vous venez d'ajouter s'affiche sous forme de lien de plage IP sous le tableau **Plage IP**.

10. Répétez les étapes 4 à 8 pour ajouter d'autres listes personnalisées.

11. Exécutez des tâches diverses présentées à l'écran.
    - Pour modifier une liste, cliquez sur le lien de la plage IP, puis modifiez les paramètres dans l'écran qui s'ouvre.
    - Pour exporter la liste dans un fichier .dat, cliquez sur **Exporter**, puis sur **Enregistrer**.
    - Si vous avez exporté une liste à partir d'un autre serveur et souhaitez l'importer dans cet écran, cliquez sur **Importer** et localisez le fichier `.dat`. La liste est chargée à l'écran.

12. Cliquez sur **Notifier tous les clients**.

Paramètres du proxy de la connexion du client

Si la connexion à Smart Protection Network nécessite l'authentification proxy, indiquez les informations d'authentification. Pour obtenir des informations détaillées, voir *Proxy externe pour les clients OfficeScan à la page 13-51*.

Configurez les paramètres de proxy interne que les clients utiliseront pour se connecter à un serveur Smart Protection Server. Pour obtenir des informations détaillées, voir *Proxy interne pour les clients OfficeScan à la page 13-50*.

Paramètres d'emplacement de l'ordinateur

OfficeScan comporte une fonction de détection d'emplacement qui identifie l'emplacement de l'ordinateur client et détermine si le client se connecte à Smart Protection Network ou à un serveur Smart Protection Server. Ceci garantit que les clients restent protégés quel que soit leur emplacement.

Pour configurer les paramètres d'emplacement, voir *Emplacement de l'ordinateur à la page 13-2*.

Installations de Trend Micro Network VirusWall

Si Trend Micro™Network VirusWall™Enforcer est installé :

- Installez un correctif de type hot fix (compilation 1047 pour Network VirusWall Enforcer 2500 et compilation 1013 pour Network VirusWall Enforcer 1200).
- Mettez à jour le moteur OPSWAT vers la version 2.5.1017 pour permettre au produit de détecter la méthode de scan d'un client.

Utilisation des services Smart Protection

Une fois l'environnement Smart Protection correctement configuré, les clients sont prêts à utiliser les services de File Reputation et de sites Web. Vous pouvez commencer à configurer les paramètres de Smart Feedback.

Remarque

Pour obtenir des instructions sur la configuration de l'environnement Smart Protection, voir *Configuration des services Smart Protection à la page 3-13*.

Afin de bénéficier de la protection fournie par les services de File Reputation, les clients doivent utiliser la méthode de scan appelée Smart Scan. Pour plus d'informations sur Smart Scan et son activation sur les clients, voir *Méthodes de scan à la page 6-8*.

Pour autoriser les clients OfficeScan à utiliser les services de réputation de sites Web, configurez les stratégies de réputation de sites Web. Pour obtenir des informations détaillées, voir *Stratégies de réputation de sites Web à la page 10-3*.

Remarque

Les paramètres des méthodes de scan et des stratégies de réputation de sites Web sont détaillés. En fonction de vos exigences, vous pouvez configurer les paramètres qui s'appliqueront à tous les clients, ou configurer des paramètres différents pour chaque client ou groupe de clients.

Pour obtenir des instructions sur la configuration de Smart Feedback, voir *Smart Feedback à la page 12-51*.

Chapitre 4

Installation du client OfficeScan

Ce chapitre décrit la configuration requise de Trend Micro™OfficeScan™ et les procédures d'installation du client OfficeScan.

Pour des instructions détaillées sur la mise à niveau des clients OfficeScan, reportez-vous au Guide d'installation et de mise à niveau d'*OfficeScan*.

Sujets abordés dans ce chapitre :

- *Installations récentes du client OfficeScan à la page 4-2*
- *Remarques relatives à l'installation à la page 4-2*
- *Éléments à prendre en compte pour le déploiement à la page 4-10*
- *Migration vers le client OfficeScan à la page 4-63*
- *Tâches après l'installation à la page 4-67*
- *Désintallation du client OfficeScan à la page 4-70*

Installations récentes du client OfficeScan

Le client OfficeScan peut être installé sur des ordinateurs exécutant les plates-formes Microsoft Windows. OfficeScan est également compatible avec de nombreux produits tiers.

Visitez le site Web suivant pour obtenir la liste complète des configurations requises et des produits tiers compatibles :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Remarques relatives à l'installation

Avant d'installer des clients, tentez compte des éléments suivants :

- **Fonctionnalités du client OfficeScan** : Des fonctionnalités du client ne sont pas disponibles sur certaines plates-formes Windows.
- **Prise en charge d'IPv6** : Le client OfficeScan peut être installé sur des clients IPv6 pur ou sur des clients à double pile. Cependant :
  - Certains systèmes d'exploitation Windows sur lesquels le client OfficeScan peut être installé ne prennent pas en charge l'adressage IPv6.
  - Pour certaines méthodes d'installation, il y a des spécifications particulières à respecter pour installer correctement le client OfficeScan.
- **Adresses IP du client OfficeScan** : Pour les clients utilisant à la fois les adressages IPv4 et IPv6, vous pouvez choisir quelle adresse sera utilisée lors de l'enregistrement du client sur le serveur.
- **Listes d'exceptions** : Assurez-vous que les listes d'exceptions pour les fonctionnalités suivantes ont été configurées correctement :
  - **Surveillance des comportements** : Ajoutez des applications nécessaires pour l'ordinateur dans la liste des Programmes approuvés pour empêcher le client OfficeScan de bloquer ces applications. Pour plus d'informations, voir *Liste d'exceptions de la surveillance des comportements à la page 7-6*.

- **Réputation de sites Web** : Ajoutez les sites Web que vous considérez sans danger à la Liste des URL approuvés pour empêcher le client OfficeScan de bloquer l'accès à ces sites Web. Pour plus d'informations, voir *Stratégies de réputation de sites Web à la page 10-3*.

Fonctionnalités du client OfficeScan

Les fonctionnalités du client OfficeScan disponibles sur un ordinateur dépendent du système d'exploitation de ce dernier.

TABLEAU 4-1. Fonctionnalités du client OfficeScan

FONCTION	SYSTÈME D'EXPLOITATION WINDOWS				
	XP	SERVEUR 2003	SERVER 2008/ SERVER CORE 2008	VISTA	7
Scan manuel, scan en temps réel et scan programmé	Oui	Oui	Oui	Oui	Oui
Mise à jour des composants (mise à jour manuelle et programmée)	Oui	Oui	Oui	Oui	Oui
Agent de mise à jour	Oui	Oui	Oui	Oui	Oui
Réputation de sites Web	Oui	Oui mais désactivé par défaut lors de l'installation du serveur	Oui mais désactivé par défaut lors de l'installation du serveur	Oui	Oui

Fonction	Système d'exploitation Windows				
	XP	Serveur 2003	Server 2008/ Server Core 2008	Vista	7
Damage Cleanup Services	Oui	Oui	Oui	Oui	Oui
Pare-feu OfficeScan	Oui	Oui mais désactivé par défaut lors de l'installation du serveur	Oui mais désactivé par défaut lors de l'installation du serveur	Oui	Oui
Surveillance des comportements	Oui (32 bits)	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (32 bits)	Oui (32 bits)
	Non (64 bits)	Non (64 bits)	Oui (64 bits) mais désactivé par défaut	Oui (64 bits) La prise en charge de Vista 64-bits requiert SP1 ou SP2	Oui (64 bits)

Fonction	Système d'exploitation Windows				
	XP	Serveur 2003	Server 2008/ Server Core 2008	Vista	7
Autoprotection client pour : • Clés de registre • Processus	Oui (32 bits)	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (32 bits)	Oui (32 bits)
	Non (64 bits)	Non (64 bits)	Oui (64 bits) mais désactivé par défaut	Oui (64 bits) La prise en charge de Vista 64-bits requiert SP1 ou SP2	Oui (64 bits)
Contrôle des dispositifs (Service de prévention des modifications non autorisées)	Oui (32 bits)	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (32 bits)	Oui (32 bits)
	Non (64 bits)	Non (64 bits)	Oui (64 bits) mais désactivé par défaut	Oui (64 bits) La prise en charge de Vista 64-bits requiert SP1 ou SP2	Oui (64 bits)

Fonction	Système d'exploitation Windows				
	XP	Serveur 2003	Server 2008/ Server Core 2008	Vista	7
Protection des données (y compris la fonction de protection des données du contrôle des dispositifs)	Oui (32 bits)	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (32 bits)	Oui (32 bits)
	Oui (64 bits)	Oui (64 bits) mais désactivé par défaut	Oui (64 bits) mais désactivé par défaut	Oui (64 bits)	Oui (64 bits)
Scan de la messagerie Microsoft Outlook	Oui (32 bits)	Oui (32 bits)	Non	Non	Non
	Non (64 bits)	Non (64 bits)			
Scan de la messagerie POP3	Oui	Oui	Oui	Oui	Oui
Prise en charge de Cisco NAC	Oui	Non	Non	Non	Non
Client Plug-in Manager	Oui	Oui	Oui	Oui	Oui
Mode itinérance	Oui	Oui	Oui (serveur) Non (Server Core)	Oui	Oui

FONCTION	SYSTÈME D'EXPLOITATION WINDOWS				
	XP	SERVEUR 2003	SERVER 2008/ SERVER CORE 2008	VISTA	7
Support SecureClient	Oui (32 bits)	Oui (32 bits)	Non	Non	Non
	Non (64 bits)	Non (64 bits)			
Smart Feedback	Oui	Oui	Oui	Oui	Oui

Installation du client OfficeScan et prise en charge d'IPv6

Cette rubrique aborde les éléments à prendre en compte lors de l'installation du client OfficeScan sur des clients IPv6 purs ou des clients à double pile.

Système d'exploitation

Le client OfficeScan ne peut être installé que sur les systèmes d'exploitation prenant en charge l'adressage IPv6 :

- Windows Vista™ (toutes les éditions)
- Windows Server 2008 (toutes les éditions)
- Windows 7 (toutes les éditions)

Visitez le site Web suivant pour obtenir la liste complète des configurations requises :

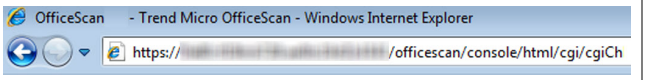
http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Méthodes d'installation

Toutes les méthodes d'installation du client OfficeScan peuvent être utilisées pour installer le client OfficeScan sur des clients IPv6 pur ou à double pile. Pour certaines méthodes d'installation, il y a des spécifications particulières à respecter pour installer correctement le client OfficeScan.

Il n'est pas possible de faire migrer ServerProtect™ vers le client OfficeScan en utilisant l'outil ServerProtect Normal Server Migration car ce dernier ne prend pas en charge l'adressage IPv6.

TABLEAU 4-2. Méthodes d'installation et prise en charge d'IPv6

MÉTHODE D'INSTALLATION	SPÉCIFICATIONS/ÉLÉMENTS À PRENDRE EN COMPTE
Page d'installation en ligne et installation sur navigateur Web	L'URL vers la page de destination comprend le nom d'hôte du serveur OfficeScan ou son adresse IP.  Si vous effectuez l'installation sur un client IPv6 pur, le serveur doit être un serveur IPv6 pur ou un serveur à double pile, et son nom d'hôte ou son adresse IPv6 doit faire partie de l'URL. Quant aux clients à double pile, l'adresse IPv6 qui s'affiche dans l'écran d'état de l'installation dépend de l'option sélectionnée dans la section **Adresse IP de votre choix** de **Ordinateurs en réseau** > **Gestion des clients**.
Client Packager	Lors de l'exécution de l'outil Client Packager, vous devrez choisir d'attribuer des privilèges d'agent de mise à jour au client. Souvenez-vous qu'un agent de mise à jour IPv6 pur ne peut distribuer des mises à jour qu'aux clients IPv6 purs ou à double pile.
Conformité de sécurité, Vulnerability Scanner, et installation à distance	Un serveur IPv6 pur ne peut pas installer le client OfficeScan sur des points finaux IPv4 pur. De même, un serveur IPv4 pur ne peut pas installer le client OfficeScan sur des points finaux IPv6 pur.

Adresses IP du client

Un serveur OfficeScan installé dans un environnement et prenant en charge l'adressage IPv6 peut gérer les clients OfficeScan suivants :

- Un serveur OfficeScan installé sur un ordinateur hôte IPv6 pur peut gérer des clients IPv6 pur.

- Un serveur OfficeScan installé sur un ordinateur hôte à double pile et auquel on a affecté des adresses IPv4 et IPv6, peut gérer des clients IPv6 pur, des clients IPv4 pur et des clients à double pile.

Après avoir installé ou mis à niveau les clients, ceux-ci s'enregistrent sur le serveur en utilisant une adresse IP.

- Les clients IPv6 pur s'enregistrent en utilisant leur adresse IPv6.
- Les clients IPv4 pur s'enregistrent en utilisant leur adresse IPv4.
- Les clients à double pile s'enregistrent en utilisant leur adresse IPv4 ou IPv6. Vous pouvez choisir l'adresse IP que ces clients utiliseront.

Configuration de l'adresse IP que les clients à double pile utilisent lors de leur enregistrement sur le serveur

Ce réglage n'est disponible que sur les serveurs OfficeScan à double pile et ne s'applique qu'aux clients à double pile.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Accédez à la section **Adresse IP de votre choix**.
3. Sélectionnez l'une des options suivantes :
   - **Uniquement IPv4** : les clients utilisent leur adresse IPv4.
   - **D'abord IPv4, ensuite IPv6**: les clients utilisent d'abord leur adresse IPv4. Si le client ne peut pas s'enregistrer en utilisant son adresse IPv4, il utilise alors son adresse IPv6. En cas d'échec de l'enregistrement avec les deux adresses IP, le client essaye à nouveau en utilisant l'ordre de priorité établi.
   - **D'abord IPv6, ensuite IPv4** : les clients utilisent d'abord leur adresse IPv6. Si le client ne peut pas s'enregistrer en utilisant son adresse IPv6, il utilise alors son adresse IPv4. En cas d'échec de l'enregistrement avec les deux adresses IP, le client essaye à nouveau en utilisant l'ordre de priorité établi.
4. Cliquez sur **Enregistrer**.

Éléments à prendre en compte pour le déploiement

Cette section donne un aperçu des différentes méthodes d'installation du client OfficeScan pour effectuer une nouvelle installation du client OfficeScan. Toutes les méthodes d'installation requièrent des droits d'administration locaux sur les ordinateurs cibles.

Si vous installez des clients et que vous souhaitez activer la prise en charge d'IPv6, consultez les instructions de la rubrique *Installation du client OfficeScan et prise en charge d'IPv6 à la page 4-7*.

TABLEAU 4-3. Considérations de déploiement de l'installation

MÉTHODE D'INSTALLATION/PRISE EN CHARGE DU SYSTÈME D'EXPLOITATION	ÉLÉMENTS À PRENDRE EN COMPTE POUR LE DÉPLOIEMENT					
	DÉPLOIEMENT SUR UN WAN	GESTION CENTRALISÉE	REQUIERT L'INTERVENTION DE L'UTILISATEUR	NÉCESSITE UNE RESSOURCE INFORMATIQUE	DÉPLOIEMENT DE MASSE	BANDE PASSANTE CONSOMMÉE
Page Web d'installation Prise en charge sur tous les systèmes d'exploitation sauf Windows Server Core 2008	Non	Non	Oui	Non	Non	Élevé
Pour initier la page d'installation basée sur le navigateur Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Élevée si les installations sont lancées simultanément

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Installations en mode UNC Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Élevée si les installations sont lancées simultanément
Depuis la page d'installation à distance Prise en charge sur tous les systèmes d'exploitation sauf : • Windows Vista Édition Familiale Basique et Édition Familiale Premium • Windows XP Édition Familiale • Windows 7 Édition Familiale Basique/Édition Familiale Premium	Non	Oui	Non	Oui	Non	Élevé

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Configuration du script de connexion Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Élevée si les installations sont lancées simultanément
Client Packager Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Faible si programmée
Client Packager (pack MSI déployé via Microsoft SMS) Prise en charge sur tous les systèmes d'exploitation	Oui	Oui	Oui/Non	Oui	Oui	Faible si programmée
Client Packager (pack MSI déployé via Active Directory) Prise en charge sur tous les systèmes d'exploitation	Oui	Oui	Oui/Non	Oui	Oui	Élevée si les installations sont lancées simultanément

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
image disque client Prise en charge sur tous les systèmes d'exploitation	Non	Non	Non	Oui	Non	Faible
Trend Micro Vulnerability Scanner (TMVS) Prise en charge sur tous les systèmes d'exploitation sauf : • Windows Vista Édition Familiale Basique et Édition Familiale Premium • Windows XP Édition Familiale	Non	Oui	Non	Oui	Non	Élevé

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Installations de la conformité de sécurité Prise en charge sur tous les systèmes d'exploitation sauf : • Windows Vista Édition Familiale Basique et Édition Familiale Premium • Windows XP Édition Familiale • Windows 7 Édition Familiale Basique/Édition Familiale Premium	Non	Oui	Non	Oui	Non	Élevé

Installations de la page Web d'installation

Les utilisateurs peuvent installer le programme client OfficeScan à partir de la page Web d'installation si vous avez installé le serveur OfficeScan sur un ordinateur fonctionnant sous les plates-formes suivantes :

- Windows Server 2003 avec Internet Information Server (IIS) 6.0 ou Apache 2.0.x
- Windows Server 2008 avec Internet Information Server (IIS) 7.0
- Windows Server 2008 R2 avec Internet Information Server (IIS) 7.5

Pour procéder à l'installation depuis la page Web d'installation, vous devez disposer des éléments suivants :

- Internet Explorer avec le niveau de sécurité défini de manière à autoriser les contrôles ActiveX™. Les versions requises sont les suivantes :
  - 6.0 sous Windows XP et Windows Server 2003
  - 7.0 sous Windows Vista et Windows Server 2008
  - 8.0 sous Windows 7
- Privilèges d'administrateur sur l'ordinateur

Pour que vos utilisateurs installent le client OfficeScan depuis la page Web d'installation, envoyez-leur les instructions suivantes. Pour envoyer une notification d'installation de client OfficeScan par e-mail, consultez *Installation basée sur un navigateur à la page 4-17*.

Installation depuis la page Web d'installation

Tâche

1. Connectez-vous à l'ordinateur à l'aide d'un compte administrateur intégré.

   Remarque

   Pour les plates-formes Windows 7, vous devez au préalable activer le compte d'administrateur intégré. Par défaut, Windows 7 désactive ce compte. Pour plus d'informations, consultez le site de l'assistance technique de Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

2. En cas d'installation sur un ordinateur fonctionnant sous Windows XP, Vista, Server 2008 ou 7, effectuez les opérations suivantes :

   a. Lancez Internet Explorer et ajoutez l'URL du serveur OfficeScan (telle que `https://<nom du serveur OfficeScan>:4343/officescan`) à la

liste des sites sécurisés. Dans Windows XP Édition Familiale, il est possible d'accéder à la liste en se rendant sous **Outils** > **Options internet** > **onglet Sécurité**, en sélectionnant l'icône **Sites de confiance** et en cliquant sur **Sites**.

b. Modifiez le paramètre de sécurité d'Internet Explorer en activant l'option **Demander confirmation pour les contrôles Active X**. Sous Windows XP, accédez à **Outils** > **Options internet** > **onglet Sécurité**, et cliquez sur **Personnaliser le niveau**.

3. Ouvrez une fenêtre Internet Explorer et saisissez l'un des éléments suivants :

   - Serveur OfficeScan avec SSL :

     ```
     https://<nom du serveur OfficeScan>:<port>/officescan
     ```

   - Serveur OfficeScan sans SSL :

     ```
     http://<nom du serveur OfficeScan>:<port>/officescan
     ```

4. Cliquez sur le lien de la page de connexion.

5. Dans le nouvel écran qui s'affiche, cliquez sur **Installer** pour démarrer l'installation du client OfficeScan. L'installation du client OfficeScan démarre. Autorisez l'installation du contrôle ActiveX quand vous y êtes invité. L'icône du client OfficeScan apparaît dans la barre d'état système de Windows après l'installation.

Remarque

Pour une liste des icônes qui s'affichent dans la barre d'état système, reportez-vous à *Icônes du client OfficeScan à la page 13-26*.

Installation basée sur le navigateur

Dans cet écran, vous pouvez définir un message électronique demandant aux utilisateurs du réseau d'installer le client OfficeScan. Pour démarrer l'installation, les utilisateurs doivent cliquer sur le lien vers le programme d'installation du client OfficeScan, fourni dans le message électronique.

Avant d'installer les clients OfficeScan :

- Vérifiez la configuration minimale requise pour l'installation du client OfficeScan.

- Identifiez les ordinateurs de votre réseau ne disposant pas d'une protection contre les risques de sécurité. Effectuez les actions suivantes :
  - Exécutez Trend Micro Vulnerability Scanner. Cet outil recherche les programmes antivirus installés sur les ordinateurs en fonction d'une plage d'adresses IP que vous spécifiez. Pour obtenir des informations détaillées, voir *Utilisation de Vulnerability Scanner à la page 4-37*.
  - Exécutez des tests de conformité de sécurité. Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les points finaux non gérés à la page 13-71*.

Installation basée sur un navigateur

Tâche

1. Accédez à **Ordinateurs en réseau** > **Installation du client** > **Basé sur navigateur**.
2. Si nécessaire, modifiez l'objet du message électronique.
3. Cliquez sur **Créer un courrier électronique.**.

   Votre programme de messagerie par défaut s'ouvre automatiquement.
4. Envoyez le message électronique aux destinataires choisis.

Exécution d'une installation basée sur UNC

`AutoPcc.exe` est un programme autonome qui installe le client OfficeScan sur les ordinateurs non protégés et met à jour les fichiers programme et les composants. Les ordinateurs doivent faire partie du domaine pour pouvoir utiliser AutoPcc via un chemin UNC (Uniform Naming Convention).

Tâche

1. Accédez à **Ordinateurs en réseau** > **Installation du client** > **En mode UNC**.
   - Pour installer le client OfficeScan sur un ordinateur non protégé à l'aide de `AutoPcc.exe` :

a. Connectez-vous au serveur. Accédez au chemin UNC :

   `\\<nom ordinateur serveur>\ofscan`

b. Cliquez avec le bouton droit de la souris sur `AutoPcc.exe` et sélectionnez **Exécuter en tant qu'administrateur**.

- Pour une installation sur un poste de travail distant à l'aide d'`AutoPcc.exe` :

  a. Ouvrez une connexion Remote Desktop Connection (Mstsc.exe) en mode console. Cela force l'installation par `AutoPcc.exe` à s'effectuer lors de la session 0.

  b. Accédez au répertoire `\\<nom ordinateur serveur>\ofscan` et exécutez `AutoPcc.exe`.

Installation à distance depuis OfficeScan Web Console

Installez le client OfficeScan à distance sur un ou plusieurs ordinateurs connectés au réseau. Vérifiez si vous disposez de droits d'administrateur sur les ordinateurs cibles pour effectuer l'installation à distance. L'outil d'installation à distance n'installe pas le client OfficeScan sur un ordinateur exécutant déjà le serveur OfficeScan.

Remarque

Cette méthode d'installation ne peut pas être employée sur les ordinateurs fonctionnant sous Windows XP Édition Familiale, ni sur ceux fonctionnant sous Windows Vista Édition Familiale Basique ou Édition Familiale Premium, ni sur ceux fonctionnant sous Windows 7 Édition Familiale Basique et Édition Familiale Premium (versions 32 bits et 64 bits). Un serveur IPv6 pur ne peut pas installer le client OfficeScan sur des clients IPv4 pur. De même, un serveur IPv4 pur ne peut pas installer le client OfficeScan sur des clients IPv6 pur.

Tâche

1. Si l'ordinateur fonctionne sous Windows Vista ou Windows 7, procédez aux étapes suivantes :

   a. Activez un compte administrateur intégré et définissez un mot de passe pour le compte.

b. Désactivez le partage de fichier simple sur le point final.

c. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils administrateurs** > **Pare-feu Windows avec fonctions avancées de sécurité**.

d. Pour Profil de domaine, Profil privé et Profil public, configurez l'état du pare-feu sur « Désactivé ».

e. Ouvrez Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter** et entrez `services.msc`) puis démarrez les services **Accès à distance**et **Appel de procédure à distance**. Lors de l'installation du client OfficeScan, utilisez le compte administrateur intégré et le mot de passe.

2. Dans la console Web, accédez à **Ordinateurs en réseau** > **Installation du client** > **Distant**.

3. Sélectionnez les ordinateurs cibles.

   - La liste **Domaines et ordinateurs** présente tous les domaines Windows du réseau. Pour afficher les ordinateurs d'un domaine, double-cliquez sur le nom du domaine. Sélectionnez un ordinateur et cliquez sur **Ajouter**.
   - Si vous souhaitez utiliser un nom d'ordinateur spécifique, saisissez le nom d'ordinateur dans le champ en haut de la page et cliquez sur **Rechercher**.

   OfficeScan vous invite à fournir le nom d'utilisateur et le mot de passe de l'ordinateur cible. Pour pouvoir continuer, assurez-vous que votre nom d'utilisateur et votre mot de passe correspondent à un compte administrateur.

4. Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.

   L'ordinateur cible apparaît dans la liste des **ordinateurs sélectionnés**.

5. Répétez les étapes 3 et 4 pour ajouter d'autres ordinateurs.

6. Cliquez sur **Installer** lorsque vous êtes prêt à installer le client OfficeScan sur les ordinateurs cibles.

   Une fenêtre de confirmation apparaît.

7. Cliquez sur **Oui** pour confirmer l'installation du client OfficeScan sur les ordinateurs cibles.

Un écran s'affiche, indiquant la progression de la copie des fichiers programme sur chaque ordinateur cible.

Lorsqu'OfficeScan a terminé l'installation sur un ordinateur cible, le nom de l'ordinateur disparaît de la liste **Ordinateurs sélectionnés** et apparaît dans la liste **Domaines et ordinateurs** avec une coche rouge.

L'installation à distance est terminée lorsque tous les ordinateurs cibles apparaissent accompagnés d'une coche rouge dans la liste **Domaines et ordinateurs**.

Remarque

Si vous exécutez l'installation sur plusieurs ordinateurs, OfficeScan enregistre tout échec dans les journaux (pour plus d'informations, voir *Journaux des nouvelles installations à la page 17-16*) tout en procédant aux autres installations. Il n'est pas nécessaire de superviser l'installation après avoir cliqué sur **Installer**. Vérifiez les journaux ultérieurement pour voir les résultats de l'installation.

Installation avec l'outil Configuration du script de connexion

L'outil Configuration du script de connexion permet d'automatiser l'installation du client OfficeScan sur les ordinateurs non protégés lorsqu'ils se connectent au réseau. Il ajoute un programme appelé `AutoPcc.exe` dans le script de connexion au serveur.

`AutoPcc.exe` installe le client OfficeScan sur les ordinateurs non protégés et met à jour les fichiers programme et les composants. Les ordinateurs doivent faire partie du domaine pour pouvoir utiliser AutoPcc à l'aide du script de connexion.

Installation du client OfficeScan

`AutoPcc.exe` installe automatiquement le client OfficeScan sur un ordinateur Windows Server 2003 non protégé lors de la connexion au serveur dont vous avez modifié les scripts de connexion. Cependant, `AutoPcc.exe` n'installe pas automatiquement le client OfficeScan sur les ordinateurs Windows 7, Vista ou Server 2008. Les utilisateurs doivent se connecter à l'ordinateur du serveur, accéder à `\\<nom de l'ordinateur du serveur>\ofcscan`, cliquer avec le bouton droit de la souris sur `AutoPcc.exe` et sélectionner **Exécuter en tant qu'administrateur**.

Pour une installation sur un poste de travail distant à l'aide d'`AutoPcc.exe` :

- L'ordinateur doit s'exécuter en mode `Mstsc.exe /console`. Cela force l'installation par `AutoPcc.exe` à s'effectuer lors de la session 0.
- Mappez un lecteur sur le dossier partagé « ofcscan » et exécutez `AutoPcc.exe` depuis cet emplacement.

Mises à jour de programmes et de composants

`AutoPcc.exe` met à jour les fichiers programme ainsi que les composants antivirus, anti-spywares et Damage Cleanup Services.

Scripts Windows Server 2003 et Windows Server 2008

Si vous disposez déjà d'un script de connexion, l'outil Configuration du script de connexion ajoute une commande permettant d'exécuter `AutoPcc.exe`. Sinon, OfficeScan crée un fichier batch appelé `ofcscan.bat` qui contient la commande d'exécution du programme `AutoPcc.exe`.

L'outil Configuration du script de connexion ajoute la ligne suivante à la fin du script :

```
\\<Server_name>\ofcscan\autopcc
```

Où :

- `<Nom_du_serveur>` correspond au nom ou à l'adresse IP de l'ordinateur sur lequel est installé le serveur OfficeScan.
- « `ofcscan` » correspond au dossier partagé OfficeScan sur le serveur.
- « `autopcc` » est le lien vers le fichier exécutable autopcc qui installe le client OfficeScan.

Emplacement du script de connexion (via un répertoire partagé Netlogon) :

- `Windows Server 2003 : \\Windows 2003 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2008 : \\Windows 2008 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

Ajout d'Autopcc.exe au script de connexion à l'aide de l'outil Configuration du script de connexion

Tâche

1. Sur l'ordinateur que vous avez utilisé pour exécuter l'installation du serveur, cliquez sur **Tous les programmes** > **Serveur OfficeScan de Trend Micro <nom du serveur>** > **Configuration du script de connexion** dans le menu Démarrer de Windows.

   L'outil **Configuration du script de connexion** se charge. La console affiche une arborescence présentant tous les domaines du réseau.

2. Recherchez le serveur dont vous souhaitez modifier le script de connexion, sélectionnez-le, puis cliquez sur **Sélectionner**. Vérifiez que ce serveur est un contrôleur de domaine principal et que vous disposez d'un accès d'administrateur à celui-ci.

   L'outil Configuration du script de connexion vous demande alors un nom d'utilisateur et un mot de passe.

3. Saisissez le nom d'utilisateur et le mot de passe. Cliquez sur **OK** pour continuer.

   La fenêtre **Sélection des utilisateurs** apparaît. La liste Utilisateurs affiche les profils des utilisateurs qui se connectent au serveur, tandis que la liste **Utilisateurs sélectionnés** affiche uniquement les profils des utilisateurs dont vous souhaitez modifier le script de connexion.

4. Pour modifier le script de connexion d'un profil utilisateur, faites votre sélection dans la liste Utilisateurs, puis cliquez sur **Ajouter**.

5. Pour modifier le script de connexion de tous les utilisateurs, cliquez sur **Ajouter tout**.

6. Pour retirer un profil utilisateur précédemment sélectionné, choisissez son nom dans la liste **Utilisateurs sélectionnés**, puis cliquez sur **Supprimer**.

7. Pour réinitialiser vos choix, cliquez sur **Supprimer tout**.

8. Cliquez sur **Appliquer** lorsque tous les profils d'utilisateurs cibles sont affichés dans la liste **Utilisateurs sélectionnés**.

Un message vous informe que vous avez modifié avec succès les différents scripts de connexion.

9. Cliquez sur **OK**.

   L'outil Configuration du script de connexion retrouve alors son aspect initial.

10. Pour modifier les scripts de connexion d'autres serveurs, répétez simplement les étapes 2 à 4.

11. Pour fermer l'outil Configuration du script de connexion, cliquez sur **Quitter**.

Installation avec Client Packager

Client Packager créé un pack d'installation que vous pouvez envoyer aux utilisateurs via des supports traditionnels tels que le CD-ROM. Les utilisateurs exécutent le pack sur l'ordinateur client pour installer ou mettre à niveau le client OfficeScan et mettre à jour les composants.

Client Packager est particulièrement utile pour déployer le client OfficeScan ou les composants vers les postes clients installés dans des bureaux distants disposant d'une faible bande passante. Les clients OfficeScan installés à l'aide de Client Packager communiquent avec le serveur sur lequel a été créé le pack d'installation.

Client Packager requiert les éléments suivants :

- 350 Mo d'espace disque disponible
- Windows Installer 2.0 (pour pouvoir exécuter un pack MSI).

Création d'un pack d'installation à l'aide de Client Packager

Tâche

1. Sur l'ordinateur du serveur OfficeScan, accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\ClientPackager`.

2. Cliquez deux fois sur le fichier `ClnPack.exe` pour exécuter l'outil. La console Client Packager s'ouvre.

3. Sélectionnez le type de pack que vous désirez créer.

TABLEAU 4-4. Types de pack client

TYPE DE PACK	DESCRIPTION
Installation	Sélectionnez **Installation** pour créer le pack sous forme de fichier exécutable. Le pack installe le programme client OfficeScan avec les composants actuellement disponibles sur le serveur. Si l'ordinateur cible dispose d'une version plus récente du client OfficeScan installée, l'exécution du fichier exécutable met à niveau le client.
Mise à jour	Sélectionnez **Mise à jour** pour créer un pack contenant les composants actuellement disponibles sur le serveur. Le pack sera créé sous forme de fichier exécutable. Utilisez ce pack si vous rencontrez des problèmes lors de la mise à jour de composants sur un ordinateur client.
MSI	Sélectionnez **MSI** pour créer un pack conforme au format de pack de Microsoft Installer. Le pack installe également le programme client OfficeScan avec les composants actuellement disponibles sur le serveur. Si l'ordinateur cible dispose d'une version plus récente du client OfficeScan installée, l'exécution du fichier MSI met à niveau le client.

4. Configurez les paramètres suivants (certains paramètres ne sont disponibles que si vous sélectionnez un type de pack particulier) :

- *Type de système d'exploitation Windows à la page 4-26*
- *Méthode de scan à la page 4-26*
- *Mode silencieux à la page 4-27*
- *Désactiver le préscan à la page 4-27*
- *Forcer l'écrasement par la dernière version à la page 4-28*
- *Fonctions de l'Agent de mise à jour à la page 4-28*
- *Scan de la messagerie Outlook à la page 4-29*
- *Support Check Point SecureClient à la page 4-29*
- *Composants à la page 4-29*

5. À côté de **Fichier source**, assurez-vous que l'emplacement du fichier `ofcscan.ini` est correct. Pour modifier le chemin, cliquez sur (...) pour accéder au fichier `ofcscan.ini`. Par défaut, ce fichier est enregistré dans le `<dossier d'installation du serveur>\PCCSRV` sur le serveur OfficeScan.

6. Dans Fichier de sortie, cliquez sur (...), spécifiez l'emplacement où vous souhaitez créer le pack client OfficeScan, ainsi que le nom de fichier (par exemple, `ClientSetup.exe`).

7. Cliquez sur **Créer**.

   Lorsque Client Packager a fini de créer le pack, le message « « Création du pack réussie » » apparaît. Recherchez le pack dans le répertoire que vous avez spécifié dans l'étape précédente.

8. Déployez le pack.

Instructions pour le déploiement du pack

1. Envoyez le pack aux utilisateurs et demandez-leur de lancer le pack client OfficeScan sur leur ordinateur en double-cliquant sur le fichier `.exe` ou `.msi`.

   Remarque

   Envoyez le pack uniquement aux utilisateurs dont le client OfficeScan dépend du serveur sur lequel le pack a été créé.

2. Si certains utilisateurs comptent installer le pack `.exe` sur des ordinateurs fonctionnant sous Windows Vista, Server 2008 ou 7, invitez-les à faire un clic droit sur le fichier `.exe`, puis à sélectionner **Exécuter en tant qu'administrateur**.

3. Si vous avez créé un fichier `.msi`, déployez le pack en effectuant les tâches suivantes :

   - Utiliser Active Directory ou Microsoft SMS. Voir *Déploiement d'un pack MSI à l'aide d'Active Directory à la page 4-30* ou *Déploiement d'un pack MSI à l'aide de Microsoft SMS à la page 4-31*.

4. Lancez le pack MSI lors de l'invite de commande pour installer le client OfficeScan en mode silencieux sur un ordinateur distant fonctionnant sous Windows XP, Vista ou Server 2008.

Type de système d'exploitation Windows

Sélectionnez le système d'exploitation pour lequel vous voulez créer le pack. Veillez à ne déployer le pack que sur des ordinateurs qui exécutent ce type de système d'exploitation. Créez un autre pack pour effectuer un déploiement sur un autre type de système d'exploitation.

Méthode de scan

Sélectionnez la méthode de scan du pack. Voir *Méthodes de scan à la page 6-8* pour obtenir des informations détaillées.

Les composants inclus dans le pack dépendent de la méthode de scan que vous avez sélectionnée. Pour plus d'informations sur les composants disponibles pour chaque méthode de scan, voir *Mise à jour des clients OfficeScan à la page 5-27*.

Avant de sélectionner la méthode de scan, prenez en compte les directives suivantes pour déployer efficacement le pack :

- Si le pack est destiné à mettre à niveau un client vers cette version d'OfficeScan, vérifiez la méthode de scan au niveau du domaine sur la console Web. Sur la console, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux**, sélectionnez le domaine de l'arborescence des clients auquel appartient le client, puis cliquez sur **Paramètres** > **Paramètres de scan** > **Méthodes de scan**. La méthode de scan du niveau domaine doit être cohérente avec celle du pack.

- Si vous prévoyez d'utiliser le pack pour effectuer une nouvelle installation du client OfficeScan, vérifiez le paramètre de regroupement des clients. Dans la console Web, accédez à **Ordinateurs en réseau** > **Regroupement des clients**.

- Si les clients sont regroupés par domaine NetBIOS, Active Directory ou DNS, vérifiez à quel domaine appartient l'ordinateur cible. Si le domaine existe, vérifiez la méthode de scan configurée pour le domaine. Si le domaine n'existe pas, vérifiez la méthode de scan du niveau racine (sélectionnez l'icône du domaine racine ( ) dans l'arborescence des clients et cliquez sur **Paramètres** > **Paramètres de scan**

> **Méthodes de scan**). La méthode de scan du domaine ou du niveau racine doit être cohérente avec celle du pack.

- Si les clients sont regroupés par groupes de clients personnalisés, vérifiez la **priorité de regroupement** et la **source**.

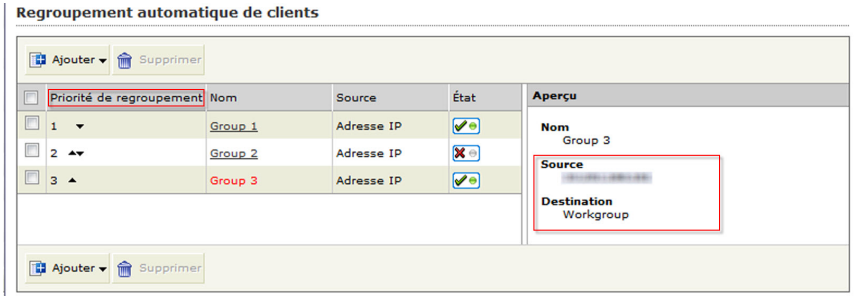


FIGURE 4-1. Volet Aperçu du regroupement automatique de clients

Si l'ordinateur cible appartient à une source spécifique, vérifiez la **destination** correspondante. La destination est indiquée par le nom de domaine apparaissant dans l'arborescence client. Une fois l'installation terminée, le client appliquera la méthode de scan propre à ce domaine.

- Si le pack est destiné à mettre à jour les composants d'un client à l'aide de cette version d'OfficeScan, vérifiez la méthode de scan configurée pour le domaine de l'arborescence des clients auquel le client appartient. La méthode de scan du niveau domaine doit être cohérente avec celle du pack.

Mode silencieux

Cette option crée un pack capable de s'installer en arrière-plan sur l'ordinateur client, de façon entièrement transparente et sans aucune fenêtre d'état de l'installation. Activez cette option si vous prévoyez de déployer le pack à distance sur l'ordinateur cible.

Désactiver le préscan

Cette option ne s'applique qu'aux installations récentes.

Si le client OfficeScan n'est pas installé sur l'ordinateur cible, le pack scanne préalablement l'ordinateur pour rechercher les risques de sécurité avant d'installer le

client OfficeScan. Si vous êtes certain que l'ordinateur cible n'est pas infecté par des risques de sécurité, désactivez le préscan.

Si le préscan est activé, le programme d'installation scanne les zones les plus vulnérables de l'ordinateur à la recherche de virus/programmes malveillants, parmi lesquelles :

- La zone et le répertoire d'amorçage (contre les virus d'amorce)
- Le dossier Windows
- Le dossier Program Files

Forcer l'écrasement par la dernière version

Cette option remplace les versions des composants sur le client par les versions actuellement disponibles sur le serveur. Activez cette option pour vous assurer que les composants du serveur et du client sont synchronisés.

Fonctions de l'Agent de mise à jour

Cette option affecte au client OfficeScan des privilèges d'agent de mise à jour sur l'ordinateur cible. Les agents de mise à jour aident le serveur OfficeScan à déployer des composants sur les clients. Pour obtenir des informations détaillées, voir *Agents de mise à jour à la page 5-55*.

Vous pouvez autoriser l'agent de mise à jour à exécuter les tâches suivantes :

- Composants de déploiement
- Paramètres de déploiement
- Programmes de déploiement

Si vous attribuez des privilèges d'agent de mise à jour à un client OfficeScan :

1. N'oubliez pas que si le pack est déployé sur un client IPv6 pur, l'agent de mise à jour ne peut distribuer des mises à jour qu'aux clients IPv6 purs ou aux clients à double pile.
2. Utilisez l'outil de configuration des mises à jour programmées pour activer et configurer les mises à jour programmées pour l'agent. Pour obtenir des informations détaillées, voir *Méthodes de mise à jour pour les agents de mise à jour à la page 5-63*.

3. Le serveur OfficeScan qui gère l'agent de mise à jour ne pourra pas synchroniser ou déployer les paramètres suivants sur l'agent :

   - Privilège d'agent de mise à jour
   - Mise à jour programmée du client
   - Mises à jour depuis le serveur ActiveUpdate de Trend Micro
   - Mises à jour depuis d'autres sources de mise à jour

   Par conséquent, déployez le pack client OfficeScan uniquement sur les ordinateurs qui ne seront pas gérés par un serveur OfficeScan. Ensuite, configurez l'agent de mise à jour pour qu'il obtienne ses mises à jour d'une source autre qu'un serveur OfficeScan, par exemple une source de mise à jour personnalisée. Si vous souhaitez que le serveur OfficeScan synchronise les paramètres avec l'agent de mise à jour, n'utilisez pas Client Packager et choisissez une autre méthode d'installation du client OfficeScan.

Scan de la messagerie Outlook

Cette option installe le programme de Scan de la messagerie Outlook, qui scanne les boîtes aux lettres Microsoft Outlook™ à la recherche de risques de sécurité. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres du scan de courrier à la page 6-62*.

Support Check Point SecureClient

Cet outil ajoute la prise en charge de Check Point™ SecureClient™ pour Windows XP et Windows Server 2003. SecureClient vérifie la version du fichier de signatures de virus avant d'autoriser la connexion au réseau. Pour obtenir des informations détaillées, voir *Aperçu général de l'architecture et de la configuration de Check Point à la page 16-2*.

Remarque

SecureClient ne vérifie pas les versions des fichiers de signatures de virus sur les clients utilisant Smart Scan.

Composants

Sélectionnez les composants et fonctionnalités à inclure dans le pack.

- Pour plus de détails sur les composants, voir *Composants et programmes OfficeScan à la page 5-2*.
- Le module Protection des données n'est disponible que si vous installez et activez la protection des données. Pour plus d'informations sur la protection des données, voir *Chapitre 9 à la page 9-1*.

Déploiement d'un pack MSI à l'aide d'Active Directory

Profitez des fonctionnalités d'Active Directory pour déployer le pack MSI sur plusieurs ordinateurs clients simultanément. Pour obtenir des instructions sur la création d'un fichier MSI, voir *Installation avec Client Packager à la page 4-23*.

Tâche

1. Effectuez les opérations suivantes :
   - Pour Windows Server 2003 et versions antérieures :
     a. Ouvrez la console Active Directory.
     b. Cliquez avec le bouton droit de la souris sur l'unité d'organisation (UO) sur laquelle vous souhaitez déployer le package MSI et cliquez sur **Propriétés**.
     c. Sous l'onglet **Stratégie de groupe**, cliquez sur **Nouveau**.
   - Pour Windows Server 2008 et Windows Server 2008 R2 :
     a. Ouvrez la console de gestion des stratégies de groupe. Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils administrateurs** > **Gestion des stratégies de groupe**.
     b. Dans l'arborescence de la console, développez **Objets de stratégie de groupe** dans la forêt et le domaine contenant l'objet de stratégie de groupe que vous souhaitez modifier.
     c. Cliquez avec le bouton droit de la souris sur l'objet de stratégie de groupe à modifier, puis cliquez sur **Modifier**. L'éditeur d'objets de stratégie de groupe s'ouvre.
2. Choisissez entre Configuration ordinateur et Configuration utilisateur et ouvrez **Paramètres du logiciel** affiché en dessous.

Conseil

Trend Micro recommande d'utiliser **Configuration ordinateur** au lieu de **Configuration utilisateur** pour garantir le succès de l'installation du pack MSI indépendamment de l'utilisateur qui se connecte à l'ordinateur.

3. Sous Paramètres du logiciel, cliquez avec le bouton droit de la souris sur **Installation de logiciel**, puis sélectionnez **Nouveau** et **Package**.
4. Déterminez l'emplacement du pack MSI et sélectionnez-le.
5. Sélectionnez une méthode de déploiement et cliquez sur **OK**.
   - **Attribué** : Le pack MSI est déployé automatiquement lors de la prochaine connexion des utilisateurs (si vous avez sélectionné Configuration utilisateur) ou lors du redémarrage de l'ordinateur (si vous avez sélectionné Configuration ordinateur). Cette méthode ne nécessite pas l'intervention de l'utilisateur.
   - **Publié** : Pour lancer le pack MSI, demandez aux utilisateurs d'accéder au Panneau de configuration, ouvrez l'écran Ajout/Suppression de programmes et sélectionnez l'option permettant d'ajouter/d'installer des programmes sur le réseau. Lorsque le pack MSI du client OfficeScan s'affiche, les utilisateurs peuvent procéder à l'installation du client OfficeScan.

Déploiement d'un pack MSI à l'aide de Microsoft SMS

Déployez le pack MSI à l'aide Microsoft SMS (System Management Server) si Microsoft BackOffice SMS est installé sur le serveur. Pour obtenir des instructions sur la création d'un fichier MSI, voir *Installation avec Client Packager à la page 4-23*.

Le serveur SMS doit obtenir le fichier MSI du serveur OfficeScan avant de pouvoir déployer le pack vers les ordinateurs cibles.

- **Local** : Le serveur SMS et le serveur OfficeScan sont sur le même ordinateur.
- **Distant** : Le serveur SMS et le serveur OfficeScan sont sur des ordinateurs différents.

Problèmes connus lors de l'installation avec Microsoft SMS :

- "Inconnu" apparaît dans la colonne Durée d'exécution de la console SMS.

- En cas d'échec de l'installation, l'état de l'installation peut indiquer que l'installation est terminée dans le moniteur de programme SMS. Pour obtenir des instructions sur la vérification de la réussite de l'installation, voir *Tâches après l'installation à la page 4-67*.

Les instructions suivantes sont valables si vous utilisez Microsoft SMS 2.0 et 2003.

Obtention d'un pack en local

Tâche

1. Ouvrez la console Administrateur SMS.
2. Sous l'onglet **Arborescence**, cliquez sur **Packages**.
3. Dans le menu **Action**, cliquez sur **Nouveau** > **Pack à partir d'une définition**.

   L'écran **Bienvenue** de l'assistant "Créer un pack à partir d'une définition" apparaît.
4. Cliquez sur **Suivant**.

   L'écran **Définition du pack** apparaît.
5. Cliquez sur **Parcourir**.

   L'écran **Ouvrir** apparaît.
6. Recherchez et sélectionnez le fichier de pack MSI créé par Client Packager, puis cliquez sur **Ouvrir**.

   Le nom du pack MSI apparaît dans l'écran **Définition du package**. Le pack affiche le « Client OfficeScan » et la version du programme.
7. Cliquez sur **Suivant**.

   L'écran **Fichiers sources** apparaît.
8. Cliquez sur **Toujours obtenir les fichiers du répertoire source**, puis sur **Suivant**.

   L'écran **Répertoire source** apparaît ; il affiche le nom du pack que vous souhaitez créer, ainsi que le répertoire source.
9. Cliquez sur **Lecteur local sur le serveur de site**.

10. Cliquez sur **Parcourir** et sélectionnez le répertoire source contenant le fichier MSI.

11. Cliquez sur **Suivant**.

    L'assistant crée le pack. Une fois le processus terminé, le nom du pack apparaît sur la console **Administrateur SMS**.

Obtention d'un pack à distance

Tâche

1. Sur le serveur OfficeScan, utilisez Client Packager pour créer un pack d'installation qui porte une extension `.exe` (vous ne pouvez pas créer de pack `.msi`). Voir *Installation avec Client Packager à la page 4-23* pour obtenir des informations détaillées.

2. Créez un dossier partagé sur l'ordinateur sur lequel vous voulez stocker la source.

3. Ouvrez la console Administrateur SMS.

4. Sous l'onglet **Arborescence**, cliquez sur **Packages**.

5. Dans le menu **Action**, cliquez sur **Nouveau** > **Pack à partir d'une définition**.

   L'écran **Bienvenue** de l'assistant "Créer un pack à partir d'une définition" apparaît.

6. Cliquez sur **Suivant**.

   L'écran **Définition du pack** apparaît.

7. Cliquez sur **Parcourir**.

   L'écran **Ouvrir** apparaît.

8. Recherchez le fichier de pack MSI. Le fichier se trouve sur le dossier partagé que vous avez créé.

9. Cliquez sur **Suivant**.

   L'écran **Fichiers sources** apparaît.

10. Cliquez sur **Toujours obtenir les fichiers du répertoire source**, puis sur **Suivant**.

    L'écran **Dossier source** apparaît.

11. Cliquez sur **Chemin d'accès au réseau (nom UNC)**.

12. Cliquez sur **Parcourir** et sélectionnez le répertoire source contenant le fichier MSI (dossier partagé précédemment créé).

13. Cliquez sur **Suivant**.

    L'assistant crée le pack. Une fois le processus terminé, le nom du pack apparaît sur la console **Administrateur SMS**.

Distribution d'un pack aux ordinateurs cibles

Tâche

1. Sous l'onglet **Arborescence**, cliquez sur **Publications**.

2. Dans le menu **Action**, cliquez sur **Toutes les tâches** > **Distribuer le programme**.

   L'écran **Bienvenue** de l'**assistant de distribution** apparaît.

3. Cliquez sur **Suivant**.

   L'écran **Pack** apparaît.

4. Cliquez sur **Sélectionner un package existant**, puis sur le nom du pack d'installation que vous avez créé.

5. Cliquez sur **Suivant**.

   L'écran **Points de distribution** apparaît.

6. Sélectionnez le point de distribution vers lequel vous souhaitez copier le pack, puis cliquez sur **Suivant**.

   L'écran **Publier un programme** apparaît.

7. Cliquez sur **Oui** pour publier le nouveau pack d'installation du client OfficeScan, puis cliquez sur **Suivant**.

   L'écran **Cible de la publication** apparaît.

8. Cliquez sur **Parcourir** pour sélectionner les ordinateurs cibles.

L'écran **Parcourir le regroupement** apparaît.

9. Cliquez sur **Tous les systèmes Windows NT**.

10. Cliquez sur **OK**.

    L'écran **Cible de la publication** apparaît à nouveau.

11. Cliquez sur **Suivant**.

    L'écran **Nom de la publication** apparaît.

12. Dans les zones de texte, entrez un nom et vos remarques concernant la publication, puis cliquez sur **Suivant**.

    L'écran **Publier dans sous-groupes** apparaît.

13. Décidez si l'annonce du nouveau pack doit ou non s'adresser aux sous-groupes. Choisissez de publier ce programme uniquement pour les membres du groupe indiqué ou pour les membres du sous-groupe.

14. Cliquez sur **Suivant**.

    L'écran **Calendrier des publications** apparaît.

15. Indiquez à quel moment publier le pack d'installation du client OfficeScan. Pour cela, saisissez ou sélectionnez la date et l'heure.

Remarque

Si vous souhaitez que Microsoft SMS cesse la publication du pack à une date précise, cliquez sur **Oui. Cette publication doit expirer**. Ensuite, indiquez la date et l'heure dans les zones **Date et heure d'expiration**.

16. Cliquez sur **Suivant**.

    L'écran **Attribuer le programme** apparaît.

17. Cliquez sur **Oui, attribuer le programme**, puis cliquez sur **Suivant**.

    Microsoft SMS génère l'annonce et l'affiche sur la console Administrateur SMS.

18. Lorsque Microsoft SMS distribue aux ordinateurs cibles le programme attribué (en l'occurrence le programme du client OfficeScan), un écran s'affiche sur chacun de

ces ordinateurs. Demandez aux utilisateurs de cliquer sur **Oui** et de suivre les instructions fournies par l'assistant afin d'installer le client OfficeScan sur leur ordinateur.

Installations à partir d'une image disque client

La technologie des images disques vous permet de créer l'image d'un client OfficeScan OfficeScan à l'aide d'un logiciel de création d'image disque et de la cloner sur les autres ordinateurs du réseau.

Chaque installation client OfficeScan requiert un identificateur global unique (GUID) permettant au serveur d'identifier les clients individuellement. Utilisez un programme OfficeScan appelé `Imgsetup.exe` pour créer un GUID différent pour chaque clone.

Création d'une image disque d'un client OfficeScan

Tâche

1. Installez le client OfficeScan sur un ordinateur.
2. Copiez `ImgSetup.exe` depuis le <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\ImgSetup` sur cet ordinateur.
3. Exécutez ensuite le fichier `ImgSetup.exe` sur l'ordinateur source.

   Ceci crée une clé de registre `RUN` sous `HKEY_LOCAL_MACHINE`.
4. Créez une image disque du client OfficeScan en utilisant le logiciel de création d'image disque.
5. Redémarrez le clone :

   `ImgSetup.exe` démarre automatiquement et crée une nouvelle valeur GUID. Le client OfficeScan communique ce nouvel identificateur au serveur, lequel crée alors un nouvel enregistrement pour le nouveau client OfficeScan.

AVERTISSEMENT!

Pour éviter que deux ordinateurs ne portent le même nom dans la base de données OfficeScan, modifiez manuellement le nom d'ordinateur ou le nom de domaine du client OfficeScan cloné.

Utilisation de Vulnerability Scanner

Vulnerability Scanner sert à détecter les solutions antivirus installées, à rechercher les ordinateurs non protégés sur votre réseau et à installer le client OfficeScan sur ces ordinateurs.

Éléments à prendre en compte lors de l'utilisation de Vulnerability Scanner

Pour déterminer si vous devez utiliser Vulnerability Scanner, tenez compte des points suivants :

- *Administration du réseau à la page 4-37*
- *Topologie et architecture du réseau à la page 4-38*
- *Spécifications logicielles/matérielles à la page 4-38*
- *Structure de domaines à la page 4-39*
- *Trafic réseau à la page 4-40*
- *Taille du réseau à la page 4-40*

Administration du réseau

TABLEAU 4-5. Administration du réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Administration avec stratégie de sécurité stricte	Très efficace. Vulnerability Scanner signale si un logiciel antivirus est installé sur tous les ordinateurs.
Responsabilité administrative distribuée sur des sites différents	Moyennement efficace

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Administration centralisée	Moyennement efficace
Service externalisé	Moyennement efficace
Les utilisateurs administrent leurs propres ordinateurs	Inefficace. Du fait que Vulnerability Scanner scanne le réseau pour vérifier les installations antivirus, il n'est pas possible que les utilisateurs scannent leur propre ordinateur.

Topologie et architecture du réseau

TABLEAU 4-6. Topologie et architecture du réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Site unique	Très efficace. Vulnerability Scanner vous permet de scanner un segment IP complet et d'installer facilement le client OfficeScan sur le réseau local.
Plusieurs sites avec connexion à haut débit	Moyennement efficace
Plusieurs sites avec connexion à bas débit	Inefficace. Vous devez exécuter Vulnerability Scanner sur chaque site et l'installation du client OfficeScan doit être dirigée vers un serveur OfficeScan local.
Ordinateurs distants et isolés	Moyennement efficace

Spécifications logicielles/matérielles

TABLEAU 4-7. Spécifications logicielles/matérielles

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Systèmes d'exploitation basés sur Windows NT	Très efficace. Vulnerability Scanner peut facilement installer le client OfficeScan à distance sur les ordinateurs qui exécutent des systèmes d'exploitation basés sur Windows NT.

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Systèmes d'exploitation mixtes	Moyennement efficace. Vulnerability Scanner peut uniquement effectuer l'installation sur les ordinateurs qui exécutent des systèmes d'exploitation basés sur Windows NT.
Logiciels de gestion des postes de travail	Inefficace. Vulnerability Scanner ne peut pas être utilisé avec les logiciels de gestion des postes de travail. Cependant, il permet de suivre l'avancement de l'installation du client OfficeScan.

Structure de domaines

TABLEAU 4-8. Structure de domaines

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Microsoft Active Directory	Très efficace. Spécifiez le compte d'administrateur de domaine dans Vulnerability Scanner pour permettre l'installation à distance du client OfficeScan.
Groupe de travail	Inefficace. Il se peut que Vulnerability Scanner ait difficultés à s'installer sur des ordinateurs utilisant des comptes d'administration et des mots de passe différents.
Novell™ Directory Service	Inefficace. Vulnerability Scanner nécessite un compte de domaine Windows pour installer le client OfficeScan.
Peer To Peer	Inefficace. Il se peut que Vulnerability Scanner ait difficultés à s'installer sur des ordinateurs utilisant des comptes d'administration et des mots de passe différents.

Trafic réseau

TABLEAU 4-9. Trafic réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Connexion en réseau local	Très efficace
512 Kbits/s	Moyennement efficace
Connexion T1 et supérieure	Moyennement efficace
RTC	Inefficace. L'installation du client OfficeScan dure un certain temps.

Taille du réseau

TABLEAU 4-10. Taille du réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Très grande entreprise	Très efficace. Plus la taille du réseau est grande, plus Vulnerability Scanner est nécessaire pour vérifier les installations du client OfficeScan.
Petites et moyennes entreprises	Moyennement efficace. Pour les réseaux de petite taille, Vulnerability Scanner peut constituer une solution pour installer le client OfficeScan. Les autres méthodes d'installations du client OfficeScan peuvent s'avérer beaucoup plus simples à mettre en œuvre.

Instructions pour l'installation du client OfficeScan avec Vulnerability Scanner

Vulnerability Scanner n'installe pas le client OfficeScan si :

- Le serveur OfficeScan ou un autre logiciel de sécurité est installé sur l'ordinateur hôte cible.
- L'ordinateur distant exécute Windows XP Édition Familiale, Windows Vista Édition Familiale Basique, Windows Vista Édition Familiale Premium, Windows 7 Édition Familiale Basique ou Windows 7 Édition Familiale Premium.

Remarque

Voous pouvez installer le client OfficeScan sur l'ordinateur hôte cible en utilisant les méthodes d'installation vues dans la rubrique *Éléments à prendre en compte pour le déploiement à la page 4-10*.

Avant d'utiliser Vulnerability Scanner pour installer le clent OfficeScan, procédez comme suit :

- Si l'ordinateur fonctionne sous Windows Vista (Professionnel, Entreprise ou Édition Intégrale) ou sous Windows 7 (Professionnel, Entreprise ou Édition Intégrale) :

  1. Activez un compte administrateur intégré et définissez un mot de passe pour le compte.
  2. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils administrateurs** > **Pare-feu Windows avec fonctions avancées de sécurité**.
  3. Pour Profil de domaine, Profil privé et Profil public, configurez l'état du pare-feu sur « Désactivé ».
  4. Ouvrez Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter**et tapez `services.msc`)puis démarrez le service **Accès à distance au Registre**. Lors de l'installation du client OfficeScan, utilisez le compte administrateur intégré et le mot de passe.

- Pour Windows XP Professionnel (versions 32 bits et 64 bits) :

  1. Ouvrez l'Explorateur Windows Explorer et cliquez sur **Outils**>**Options des dossiers**.
  2. Cliquez sur l'onglet **Affichage** et désactivez **Utiliser le partage de fichiers simple (recommandé)**.

Méthodes de vulnerability scan

Les scans de vulnérabilité vérifient la présence de logiciels de sécurité sur les ordinateurs hôtes et peut installer le client OfficeScan sur les ordinateurs non protégés.

Il existe plusieurs façons d'exécuter un vulnerability scan.

TABLEAU 4-11. Méthodes de vulnerability scan

MÉTHODE	DÉTAILS
Vulnerability scan manuel	Les administrateurs peuvent effectuer des scans de vulnérabilité sur demande.
Scan DHCP	Les administrateurs peuvent effectuer des scans de vulnérabilité sur des ordinateurs hôtes qui demandent des adresses IP à un serveur DHCP. Vulnerability Scanner écoute sur le port 67 qui est le port d'écoute du serveur DHCP pour les requêtes DHCP. S'il détecte une requête DHCP provenant d'un ordinateur hôte, un vulnerability scan s'exécute sur l'ordinateur. **Remarque** Vulnerability Scanner ne peut pas détecter de requêtes DHCP si vous l'avez exécuté sur Windows Server 2008 ou Windows 7.
Vulnerability scan programmé	Des scans de vulnérabilité sont automatiquement exécutés en fonction du programme configuré par les administrateurs.

Une fois Vulnerability Scanner lancé, l'état du client OfficeScan sur les ordinateurs hôtes cibles s'affiche. L'état peut être :

- **Normal** : le client OfficeScan est opérationnel et fonctionne correctement
- **Anormal** : les services du client OfficeScan ne fonctionnent pas ou le client n'a pas de protection en temps réel
- **Non installé** : Le service TMListen est manquant ou le client OfficeScan n'a pas été installé
- **Inaccessible** : Vulnerability Scanner n'a pas réussi à établir la connexion avec la machine hôte et à déterminer l'état du client OfficeScan

Exécution d'un scan manuel de Vulnerability

Tâche

1. Pour exécuter un scan de vulnérabilité sur l'ordinateur serveur OfficeScan, accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS` et double-cliquez sur `TMVS.exe`. La console Trend Micro Vulnerability Scanner apparaît. Pour effectuer un vulnerability scan sur un autre ordinateur fonctionnant sous Windows XP, Server 2003, Server 2008, Vista ou 7 :

   a. Sur l'ordinateur serveur OfficeScan, accédez au `<dossier d'installation du serveur >\PCCSRV\Admin\Utility`.

   b. Copiez le dossier `TMVS` sur l'autre ordinateur.

   c. Sur l'autre ordinateur, ouvrez le dossier `TMVS` et exécutez `TMVS.exe`.

      La console **Trend Micro Vulnerability Scanner** apparaît.

   Remarque

   Vous ne pouvez pas lancer l'outil à partir de Terminal Server.

2. Rendez-vous à la section **Scan manuel**.

3. Saisissez la plage d'adresses IP des ordinateurs que vous souhaitez vérifier.

   a. Saisissez une plage d'adresses IPv4.

   Remarque

   Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv4 s'il est exécuté sur un ordinateur IPv4 pur ou à double-pile. Vulnerability Scanner prend uniquement en charge les plages d'adresses IP de la classe B, par exemple 168.212.1.1 à 168.212.254.254.

   b. Pour une plage d'adresses IPv6, saisissez le préfixe IPv6 et la longueur du préfixe.

Remarque

Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv6 s'il est exécuté sur un ordinateur hôte IPv6 pur ou à double-pile.

4. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.

5. Configurez les paramètres suivants :

   a. **Paramètres de ping** : un vulnerability scan peut envoyer des requêtes « ping » aux adresses IP spécifiées précédemment pour vérifier si elles sont en cours d'utilisation. Si un ordinateur hôte cible utilise une de ces adresses IP, Vulnerability Scanner peut déterminer le système d'exploitation de l'ordinateur hôte. Pour obtenir des informations détaillées, voir *Paramètres de ping à la page 4-58*.

   b. **Méthode de récupération des descriptions d'ordinateurs** : Vulnerability Scanner peut récupérer des informations complémentaires concernant les ordinateurs hôtes qui répondent à la commande « ping ». Pour obtenir des informations détaillées, voir *Méthode de récupération des descriptions d'ordinateurs à la page 4-55*.

   c. **Recherche de produits** : Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Recherche de produits à la page 4-52*.

   d. **Paramètres du serveur OfficeScan** : Configurez ces paramètres si vous souhaitez que Vulnerability Scanner installe automatiquement le client OfficeScan sur les ordinateurs hôtes distants. Ces paramètres identifient le serveur parent du client OfficeScan et les informations d'authentification d'administration utilisées pour se connecter aux ordinateurs hôtes. Pour obtenir des informations détaillées, voir *Paramètres du serveur OfficeScan à la page 4-59*.

Remarque

Certaines conditions peuvent empêcher l'installation du client OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation du client OfficeScan avec Vulnerability Scanner à la page 4-40*.

e. **Notifications** : Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés. Pour obtenir des informations détaillées, voir *Notifications à la page 4-56*.

f. **Enregistrer les résultats** : En plus d'envoyer les résultats du vulnerability scan aux administrateurs, Vulnerability Scanner peut également enregistrer les résultats du scan dans un fichier `.csv`. Pour obtenir des informations détaillées, voir *Résultats de Vulnerability Scan à la page 4-57*.

6. Cliquez sur **OK**.

   L'écran Paramètres se ferme.

7. Cliquez sur **Start**.

   Les résultats du scan des failles s'affichent dans le tableau **Résultats** sous l'onglet **Scan manuel**.

Remarque

Les informations d'adresse MAC ne s'affichent pas dans la table **Résultats** si l'ordinateur exécute Windows Server 2008.

8. Pour enregistrer les résultats dans un fichier au format CSV (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Exécution d'un scan DHCP

Tâche

1. Configurez les paramètres DHCP dans le fichier `TMVS.ini` qui se trouve dans le dossier suivant : <*Dossier d'installation du server*>`\PCCSRV\Admin\Utility\TMVS`.

TABLEAU 4-12. Paramètres DHCP dans le fichier `TMVS.ini`

PARAMÈTRE	DESCRIPTION
DhcpThreadNum=x	Spécifiez le numéro de thread pour le mode DHCP. La valeur minimale est 3 et la valeur maximale 100. La valeur par défaut est 3.
DhcpDelayScan=x	C'est le délai d'attente en secondes avant que ne soit vérifié sur l'ordinateur demandeur si le logiciel antivirus est installé. La valeur minimale est 0 (aucune attente) et la valeur maximale 600. La valeur par défaut est 60.
LogReport=x	0 désactive l'écriture dans le journal et 1 l'active. Vulnerability Scanner envoie les résultats du scan au serveur OfficeScan. Les journaux s'affichent dans l'écran **Journaux des événements du système** de la console Web.
OsceServer=x	Adresse IP ou nom DNS du serveur OfficeScan.
OsceServerPort=x	Port du serveur Web sur le serveur OfficeScan.

2. Pour exécuter un scan de vulnérabilité sur l'ordinateur serveur OfficeScan, accédez au `<dossier d'installation du serveur >\PCCSRV\Admin\Utility\TMVS` et double-cliquez sur `TMVS.exe`. La console **Trend Micro Vulnerability Scanner** apparaît.

   a. Sur l'ordinateur serveur OfficeScan, accédez au `<dossier d'installation du serveur >\PCCSRV\Admin\Utility`.

   b. Copiez le dossier `TMVS` sur l'autre ordinateur.

   c. Sur l'autre ordinateur, ouvrez le dossier `TMVS` et exécutez `TMVS.exe`.

      La console **Trend Micro Vulnerability Scanner** apparaît.

Remarque

Vous ne pouvez pas lancer l'outil à partir de Terminal Server.

3. Dans la section **Scan manuel**, cliquez sur **Paramètres**.

L'écran **Paramètres** apparaît.

4. Configurez les paramètres suivants :

   a. **Recherche Produits** : Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Recherche de produits à la page 4-52*.

   b. **Paramètres de serveur OfficeScan** : configurez ces paramètres si vous souhaitez que Vulnerability Scanner installe automatiquement le client OfficeScan sur les ordinateurs hôtes distants. Ces paramètres identifient le serveur parent du client OfficeScan et les informations d'authentification d'administration utilisées pour se connecter aux ordinateurs hôtes. Pour obtenir des informations détaillées, voir *Paramètres du serveur OfficeScan à la page 4-59*.

   Remarque

   Certaines conditions peuvent empêcher l'installation du client OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation du client OfficeScan avec Vulnerability Scanner à la page 4-40*.

   c. **Notifications**: Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés. Pour obtenir des informations détaillées, voir *Notifications à la page 4-56*.

   d. **Enregistrer les résultats** : en plus d'envoyer des résultats du vulnerability scan aux administrateurs, Vulnerability Scanner peut également enregistrer les résultats dans un fichier `.csv`. Pour obtenir des informations détaillées, voir *Résultats de Vulnerability Scan à la page 4-57*.

5. Cliquez sur **OK**.

   L'écran Paramètres se ferme.

6. Dans la table **Résultats**, cliquez sur l'onglet **Scan DHCP**.

Remarque

L'onglet **Scan DHCP** n'est pas disponible sur les ordinateurs exécutant Windows Server 2008 et Windows 7.

7. Cliquez sur **Start**.

   Vulnerability scanner commence à écouter les requêtes DHCP et à exécuter les contrôles de failles sur les ordinateurs au fur et à mesure qu'ils se connectent au réseau.

8. Pour enregistrer les résultats dans un fichier au format CSV (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Configuration d'un scan Vulnerability programmé

Tâche

1. Pour exécuter un scan de vulnérabilité sur l'ordinateur serveur OfficeScan, accédez au <*dossier d'installation du serveur* >`\PCCSRV\Admin\Utility\TMVS` et double-cliquez sur `TMVS.exe`. La console **Trend Micro Vulnerability Scanner** apparaît. Pour effectuer un vulnerability scan sur un autre ordinateur fonctionnant sous Windows XP, Server 2003, Server 2008, Vista ou 7 :

   a. Sur l'ordinateur serveur OfficeScan, accédez au `<dossier d'installation du serveur >\PCCSRV\Admin\Utility`.

   b. Copiez le dossier `TMVS` sur l'autre ordinateur.

   c. Sur l'autre ordinateur, ouvrez le dossier `TMVS` et exécutez `TMVS.exe`.

      La console **Trend Micro Vulnerability Scanner** apparaît.

Remarque

Vous ne pouvez pas lancer l'outil à partir de Terminal Server.

2. Rendez-vous à la section **Scan programmé**.

3. Cliquez sur **Ajouter/Modifier**.

L'écran **Scan programmé** apparaît.

4. Configurez les paramètres suivants :

   a. **Nom**: entrez le nom du vulnerability scan programmé.

   b. **Plage d'adresses IP**: Saisissez la plage d'adresses IP des ordinateurs que vous souhaitez vérifier.

      i. Saisissez une plage d'adresses IPv4.

      Remarque

      Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv4 s'il est exécuté sur un ordinateur hôte IPv4 pur ou à double pile qui a une adresse IPv4 disponible. Vulnerability Scanner prend uniquement en charge les plages d'adresses IP de la classe B, par exemple 168.212.1.1 à 168.212.254.254.

      ii. Pour une plage d'adresses IPv6, saisissez le préfixe IPv6 et la longueur du préfixe.

      Remarque

      Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv6 s'il est exécuté sur un ordinateur hôte IPv6 pur ou à double pile qui a une adresse IPv6 disponible.

   c. **Programmation** : spécifiez l'heure de démarrage en utilisant le format 24 heures, puis sélectionnez la fréquence des scans. Choisissez s'il doit être quotidien, hebdomadaire ou mensuel.

   d. **Paramètres**: Sélectionnez quel ensemble de paramètres de vulnerability scan utiliser.

      - Sélectionnez **Utiliser les paramètres en cours** si vous avez configuré les paramètres de vulnerability scan manuel et que vous souhaitez les utiliser. Pour plus de détails sur les paramètres de vulnerability scan manuel, voir *Exécution d'un scan manuel de Vulnerability à la page 4-43*.

      - Si vous n'avez pas spécifié de paramètres de vulnerability scan manuel ou que vous souhaitez utiliser un autre ensemble de paramètres,

sélectionnez **Modifier les paramètres**, puis cliquez sur **Paramètres**. L'écran **Paramètres** apparaît.

Vous pouvez configurer les paramètres suivants, puis cliquez sur **OK** :

- **Paramètres de ping**: Un vulnerability scan peut envoyer des requêtes « ping » aux adresses IP spécifiées à l'étape 4b pour vérifier si elles sont en cours d'utilisation. Si un ordinateur hôte cible utilise une de ces adresses IP, Vulnerability Scanner peut déterminer le système d'exploitation de l'ordinateur hôte. Pour obtenir des informations détaillées, voir *Paramètres de ping à la page 4-58*.

- **Méthode de récupération des descriptions d'ordinateurs** : Vulnerability Scanner peut récupérer des informations complémentaires concernant les ordinateurs hôtes qui répondent à la commande « ping ». Pour obtenir des informations détaillées, voir *Méthode de récupération des descriptions d'ordinateurs à la page 4-55*.

- **Recherche de produits** : Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Recherche de produits à la page 4-52*.

- **Paramètres du serveur OfficeScan** : configurez ces paramètres si vous souhaitez que Vulnerability Scanner installe automatiquement le client OfficeScan sur les ordinateurs hôtes distants. Ces paramètres identifient le serveur parent du client OfficeScan et les informations d'authentification d'administration utilisées pour se connecter aux ordinateurs hôtes. Pour obtenir des informations détaillées, voir *Paramètres du serveur OfficeScan à la page 4-59*.

Remarque

Certaines conditions peuvent empêcher l'installation du client OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation du client OfficeScan avec Vulnerability Scanner à la page 4-40*.

- **Notifications** : Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également

afficher des notifications sur les ordinateurs hôtes non protégés. Pour obtenir des informations détaillées, voir *Notifications à la page 4-56*.

- **Enregistrer les résultats** : En plus d'envoyer les résultats du vulnerability scan aux administrateurs, Vulnerability Scanner peut également enregistrer les résultats du scan dans un fichier .csv. Pour obtenir des informations détaillées, voir *Résultats de Vulnerability Scan à la page 4-57*.

5. Cliquez sur **OK**.

   L'écran **Scan programmé** se ferme. Le vulnerability scan programmé que vous avez créé apparaît sous la section **Scan programmé**. Si vous avez activé les notifications, Vulnerability Scanner vous envoie les résultats du vulnerability scan programmé.

6. Pour exécuter immédiatement le vulnerability scan programmé, cliquez sur **Exécuter maintenant**.

   Les résultats du vulnerability scan s'affichent dans le tableau **Résultats** sous l'onglet **Scan programmé**.

   Remarque

   Les informations d'adresse MAC ne s'affichent pas dans la table **Résultats** si l'ordinateur exécute Windows Server 2008.

7. Pour enregistrer les résultats dans un fichier au format `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Paramètres de Vulnerability Scan

La configuration des paramètres de vulnerability scan s'effectue à partir de Trend Micro Vulnerability Scanner (`TMVS.exe`) ou du fichier `TMVS.ini`.

Remarque

Reportez-vous à *Journaux de débogage du serveur à l'aide de LogServer.exe à la page 17-3* pour savoir comment collecter des journaux pour Vulnerability Scanner.

Recherche de produits

Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les clients. Le tableau suivant explique comment Vulnerability Scanner vérifie la présence de produits de sécurité :

TABLEAU 4-13. Produits de sécurité vérifiés par Vulnerability Scanner

PRODUIT	DESCRIPTION
ServerProtect for Windows	Vulnerability Scanner utilise le point final RPC pour vérifier si `SPNTSVC.exe` est en cours d'exécution. Il renvoie des informations telles que le système d'exploitation, le moteur de scan antivirus, le fichier de signatures de virus et les versions du produit. Vulnerability Scanner ne peut pas détecter le serveur d'informations ServerProtect ou la console de gestion ServerProtect.
ServerProtect for Linux	Si l'ordinateur cible n'exécute pas Windows, Vulnerability Scanner vérifie si ServerProtect for Linux est installé sur celui-ci en essayant de se connecter au port 14942.
Client OfficeScan	Vulnerability Scanner utilise le port du client OfficeScan pour vérifier si le client OfficeScan est installé. Il vérifie également si le processus `TmListen.exe` est en cours d'exécution. Il extrait automatiquement le numéro de port s'il est exécuté à partir de son emplacement par défaut. Si vous avez lancé Vulnerability Scanner sur un ordinateur autre que le serveur OfficeScan, vérifiez puis utilisez le port de communication de l'autre ordinateur.
PortalProtect™	Vulnerability Scanner charge la page Web `http://localhost:port/PortalProtect/index.html` afin de vérifier l'installation du produit.

PRODUIT	DESCRIPTION
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner charge la page Web `http://ipaddress:port/scanmail.html` afin de vérifier l'installation de ScanMail.. Par défaut, ScanMail utilise le port 16372. Si ScanMail utilise un autre numéro de port, spécifiez-le. Sinon, Vulnerability Scanner ne pourra pas détecter ScanMail.
Gamme™ InterScan	Vulnerability Scanner charge les pages Web de différents produits pour vérifier leur installation. • InterScan Messaging Security Suite 5.x : `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x : `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x : `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner utilise le port 40116 pour vérifier si Trend Micro Internet Security est installé.
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner envoie un jeton spécial au port TCP port 8081, le port par défaut de ePolicy Orchestrator pour fournir la connexion entre le serveur et le client. L'ordinateur possédant ce produit antivirus répond en utilisant un type de jeton spécial. Vulnerability Scanner ne peut pas détecter la version autonome de McAfee VirusScan.
Norton Antivirus™ Corporate Edition	Vulnerability Scanner envoie un jeton spécial au port UDP port 2967, le port par défaut de Norton Antivirus Corporate Edition RTVScan. L'ordinateur possédant ce produit antivirus répond en utilisant un type de jeton spécial. Comme Norton Antivirus Corporate Edition communique via UDP, le taux de précision n'est pas garanti. De plus, le trafic réseau peut influer sur le temps d'attente UDP.

Vulnerability Scanner détecte les produits et les ordinateurs à l'aide des protocoles suivants :

- **RPC**: pour détecter ServerProtect for NT.
- **UDP**: pour détecter les clients de Norton AntiVirus Corporate Edition.

- **TCP**: pour détecter McAfee VirusScan ePolicy Orchestrator.
- **ICMP**: pour détecter les ordinateurs en envoyant les paquets ICMP.
- **HTTP** : pour détecter les clients d'OfficeScan.
- **DHCP**: s'il détecte une requête DHCP, Vulnerability Scanner vérifie si un logiciel antivirus a déjà été installé sur l'ordinateur demandeur.

Configuration des paramètres Product Query

Les paramètres de recherche de produits sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 4-41*.

Tâche

1. Pour définir les paramètres de recherche de produits à partir de Vulnerability Scanner (`TMVS.exe`) :
   a. Exécutez `TMVS.exe`.
   b. Cliquez sur **Settings**.
      L'écran **Paramètres** apparaît.
   c. Rendez-vous à la section **Recherche de produit**.
   d. Sélectionnez les produits à vérifier.
   e. Cliquez sur **Paramètres** en regard du nom d'un produit, puis spécifiez le numéro de port qui sera vérifié par Vulnerability Scanner.
   f. Cliquez sur **OK**.
      L'écran **Paramètres** se ferme.
2. Pour définir le nombre d'ordinateurs que Vulnerability Scanner vérifie simultanément à la recherche d'un programme antivirus :
   a. Accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS` et ouvrez `TMVS.ini` à l'aide d'un éditeur de texte tel que le Bloc-notes.

b. Pour définir le nombre d'ordinateurs vérifiés lors de scans de vulnérabilité manuels, modifiez la valeur `ThreadNumManual`. Indiquez une valeur comprise entre 8 et 64.

   Saisissez par exemple `ThreadNumManual=60` pour que Vulnerability Scanner vérifie 60 ordinateurs en même temps.

c. Pour définir le nombre d'ordinateurs vérifiés lors de scans de vulnérabilité programmés, modifiez la valeur `ThreadNumSchedule`. Indiquez une valeur comprise entre 8 et 64.

   Saisissez par exemple `ThreadNumSchedule=50` pour que Vulnerability Scanner vérifie 50 ordinateurs en même temps.

d. Enregistrez le fichier `TMVS.ini`.

Méthode de récupération des descriptions d'ordinateurs

Losrque Vulnerability Scanner est est mesure d'envoyer une requête « ping » aux ordinateurs hôtes, il peut récupérer des informations complémentaires concernant les ordinateurs hôtes. Il existe deux méthodes de récupération des informations :

- **Récupération rapide** : ne récupère que le nom de l'ordinateur
- **Récupération normale** : récupère à la fois les informations relatives au domaine et à l'ordinateur

Configuration des paramètres de récupération

Les paramètres de récupération sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 4-41*.

Tâche

1. Exécutez `TMVS.exe`.
2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.

3. Rendez-vous à la section **Méthode de récupération des descriptions d'ordinateurs**.
4. Sélectionnez **Normale** ou **Rapide**.
5. Si vous avez sélectionné **Normal**, sélectionnez **Récuperer les descriptions d'ordinateurs si elles sont disponibles**.
6. Cliquez sur **OK**.

   L'écran **Paramètres** se ferme.

Notifications

Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés.

Configuration des paramètres de notification

Les paramètres de notification sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 4-41*.

Tâche

1. Exécutez `TMVS.exe`.
2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.
3. Rendez-vous à la section **Notifications**.
4. Pour envoyer automatiquement les résultats de vulnerability scan à vous-même ou à d'autres administrateurs de votre entreprise :

   a. Sélectionnez **Envoyer les résultats par courrier électronique à l'administrateur système**.

   b. Cliquez sur **Configurer** pour spécifier les paramètres de courrier électronique.

c. Saisissez l'adresse e-mail du destinataire dans **À**.

d. Saisissez l'adresse e-mail de l'expéditeur dans **De**.

e. Entrez l'adresse du serveur SMTP dans **Serveur SMTP**.

Saisissez par exemple `société.smtp.com`. Les informations relatives au serveur SMTP sont obligatoires.

f. Sous **Objet**, entrez un nouvel objet pour le message ou acceptez l'objet par défaut.

g. Cliquez sur **OK**.

5. Pour informer les utilisateurs que leurs ordinateurs n'ont aucun logiciel de sécurité installé :

a. Sélectionnez **Afficher une notification sur les ordinateurs non protégés**.

b. Cliquez sur **Personnaliser** pour configurer le message de notification.

c. Dans l'écran **Message de notification**, entrez un nouveau message ou acceptez le message par défaut.

d. Cliquez sur **OK**.

6. Cliquez sur **OK**.

L'écran **Paramètres** se ferme.

Résultats de Vulnerability Scan

Vous pouvez configurer Vulnerability Scanner pour qu'il enregistre les résultats de vulnerability scan en tant que fichier CSV (valeurs séparées par des virgules).

Configuration des résultats de scan

Les paramètres de résultats de vulnerability scan sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 4-41*.

Tâche

1. Exécutez `TMVS.exe`.
2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.
3. Rendez-vous à la section **Enregistrer les résultats**.
4. Sélectionnez **Enregistrer automatiquement les résultats dans un fichier CSV**.
5. Pour modifier le dossier d'enregistrement du fichier `CSV` :
   a. Cliquez sur **Parcourir**.
   b. Sélectionnez un dossier cible sur l'ordinateur ou sur le réseau.
   c. Cliquez sur **OK**.
6. Cliquez sur **OK**.

   L'écran **Paramètres** se ferme.

Paramètres de ping

Utilisez les paramètres de « ping » pour confirmer l'existence d'un ordinateur cible et déterminer son système d'exploitation. Si ces paramètres sont désactivés, Vulnerability Scanner scanne toutes les adresses IP dans la plage d'adresses IP (même celles qui ne sont utilisées sur aucun ordinateur), ce qui rend la tentative de scan plus longue qu'elle ne devrait l'être.

Configuration des paramètres Ping

Les paramètres de ping sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 4-41*.

Tâche

1. Pour définir les paramètres de ping à partir de Vulnerability Scanner (`TMVS.exe`) :

a. Exécutez `TMVS.exe`.

b. Cliquez sur **Settings**.

L'écran **Paramètres** apparaît.

c. Rendez-vous à la section **Paramètres de ping**.

d. Sélectionnez **Permettre à Vulnerability Scanner d'envoyer une requête ping aux ordinateurs du réseau pour vérifier leur état**.

e. Acceptez ou modifiez les valeurs des champs **Taille des paquets** et **Expiration**.

f. Sélectionnez **Détecter le type de SE par le système de reconnaissance de SE**.

Si vous sélectionnez cette option, Vulnerability Scanner détermine si un ordinateur hôte fonctionne sous Windows ou sous un autre système d'exploitation. Pour des ordinateurs hôtes fonctionnant sous Windows, Vulnerability Scanner peut identifier la version de Windows.

g. Cliquez sur **OK**.

L'écran **Paramètres** se ferme.

2. Pour définir le nombre d'ordinateurs auquel Vulnerability Scanner envoie simultanément une requête ping :

a. Accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS` et ouvrez `TMVS.ini` à l'aide d'un éditeur de texte tel que le Bloc-notes.

b. Modifiez la valeur d'`EchoNum`. Indiquez une valeur comprise entre 1 et 64.

Saisissez par exemple `EchoNum=60` pour que Vulnerability Scanner envoie une requête ping à 60 ordinateurs en même temps.

c. Enregistrez le fichier `TMVS.ini`.

Paramètres du serveur OfficeScan

Les paramètres de serveur OfficeScan sont utilisés lorsque :

- Vulnerability Scanner installe le client OfficeScan sur les ordinateurs cibles non protégés. Les paramètres de serveur permettent à Vulnerability Scanner d'identifier le serveur parent du client OfficeScan ainsi que les informations d'authentification d'administration à utiliser lors d'une connexion aux ordinateurs cibles.

  Remarque

  Certaines conditions peuvent empêcher l'installation du client OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation du client OfficeScan avec Vulnerability Scanner à la page 4-40*.

- Vulnerability Scanner envoie les journaux d'installation du client au serveur OfficeScan.

Configuration des paramètres du serveur OfficeScan

Les paramètres de serveur OfficeScan sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 4-41*.

Tâche

1. Exécutez `TMVS.exe`.
2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.
3. Rendez-vous à la section **Paramètres de serveur OfficeScan**.
4. Tapez le nom et le numéro de port du serveur OfficeScan.
5. Sélectionnez **Installation automatique du client OfficeScan sur les ordinateurs non protégés**.
6. Pour configurer les informations d'authentification d'administration :
   a. Cliquez sur **Installation du compte**.
   b. Sur l'écran **Informations de compte**, entrez un nom d'utilisateur et un mot de passe.
   c. Cliquez sur **OK**.

7. Sélectionnez **Envoi des journaux au serveur OfficeScan**.
8. Cliquez sur **OK**.

   L'écran **Paramètres** se ferme.

Installation avec la conformité à la sécurité

Vous pouvez installer les clients OfficeScan sur des ordinateurs appartenant aux domaines du réseau ou installer le client OfficeScan sur un ordinateur cible en utilisant son adresse IP.

Avant d'installer le client OfficeScan, veillez à suivre les consignes ci-après :

Tâche

1. Notez les informations de connexion de chaque ordinateur. OfficeScan vous invitera à les spécifier pendant l'installation.
2. Le client OfficeScan ne sera pas installé sur un ordinateur si :
   - Le serveur OfficeScan est installé sur l'ordinateur.
   - L'ordinateur exécute Windows XP Édition Familiale, Windows Vista Édition Familiale Basique, Windows Vista Édition Familiale Premium, Windows 7™ Édition Starter, Windows 7 Édition Familiale Basique ou Windows 7 Édition Familiale Premium. Si vous disposez d'ordinateurs exécutant ces plates-formes, choisissez une autre méthode d'installation. Voir *Éléments à prendre en compte pour le déploiement à la page 4-10* pour obtenir des informations détaillées.
3. Si l'ordinateur cible fonctionne sous Windows Vista (Professionnel, Entreprise ou Édition Intégrale) ou Windows 7 (Professionnel, Entreprise ou Édition Intégrale), effectuez la procédure suivante sur l'ordinateur :
   a. Activez un compte administrateur intégré et définissez un mot de passe pour le compte.
   b. Désactivez le pare-feu Windows.
   c. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils administrateurs** > **Pare-feu Windows avec fonctions avancées de sécurité**.

d. Pour Profil de domaine, Profil privé et Profil public, configurez l'état du pare-feu sur « Désactivé ».

e. Ouvrez Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter** et tapez `services.msc`) puis démarrez le service **Accès à distance au Registre**. Lors de l'installation du client OfficeScan, utilisez le compte administrateur intégré et le mot de passe.

4. Si des programmes de sécurité de point final Trend Micro ou tiers sont installés sur l'ordinateur, vérifiez si OfficeScan peut les désinstaller automatiquement et les remplacer par le client OfficeScan. Pour obtenir la liste des logiciels de sécurité pour clients qu'OfficeScan désinstalle automatiquement, ouvrez les fichiers suivants dans le <*dossier d'installation du serveur*>`\PCCSRV\Admin`. Vous pouvez ouvrir ces fichiers à l'aide d'un éditeur de texte comme le Bloc-notes.

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   Si le logiciel de l'ordinateur cible n'est pas inclus dans la liste, désinstallez-le d'abord manuellement. En fonction du processus de désinstallation du logiciel, l'ordinateur procédera ou non à un redémarrage après la désinstallation.

Installation du client OfficeScan

Tâche

1. Accédez à **Conformité de la sécurité** > **Gestion des serveurs externes**.
2. Cliquez sur **Installer** en haut de l'arborescence des clients.

   - Si une version moins récente du client OfficeScan est déjà installée sur un ordinateur et que vous cliquez sur **Installer**, l'installation sera ignorée et le client ne sera pas mis à niveau vers cette version. Pour mettre à niveau le client, un paramètre doit être désactivé.

     a. Accédez à l'**Ordinateurs en réseau** > **Gestion des clients**.

     b. Cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.

c. Désactivez l'option **Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client ni déployer des correctifs de type hot fix**.

3. Spécifiez le compte de connexion d'administrateur pour chaque ordinateur et cliquez sur **Connexion**. OfficeScan commence à installer le client sur l'ordinateur cible.

4. Affichez l'état de l'installation.

Migration vers le client OfficeScan

Remplacez le logiciel de sécurité du client installé sur un ordinateur cible par le client OfficeScan.

Migration à partir d'autres logiciels de sécurité de points finaux

Lorsque vous installez le client OfficeScan, le programme d'installation recherche les logiciels de sécurité de points finaux Trend Micro ou tiers installés sur l'ordinateur cible. Le programme d'installation du client peut désinstaller automatiquement les logiciels et les remplacer par le client OfficeScan.

Pour obtenir la liste des logiciels de sécurité pour points finaux qu'OfficeScan désinstalle automatiquement, ouvrez les fichiers suivants dans le <*dossier d'installation du serveur*>`\PCCSRV\Admin`. Ouvrez ces fichiers à l'aide d'un éditeur de texte comme le Bloc-notes.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

Si le logiciel de l'ordinateur cible n'est pas inclus dans la liste, désinstallez-le d'abord manuellement. En fonction du processus de désinstallation du logiciel, l'ordinateur procédera ou non à un redémarrage après la désinstallation.

Problèmes de migration des clients OfficeScan

- Si la migration automatique des clients est réussie alors qu'un utilisateur rencontre un problème avec le client OfficeScan juste après l'installation, redémarrez l'ordinateur.
- Si le programme d'installation d'OfficeScan effectuait l'installation du client OfficeScan sans être en mesure de désinstaller l'autre logiciel de sécurité, il y aurait des conflits entre les deux logiciels. Désinstallez les deux logiciels, puis installez le client OfficeScan à l'aide d'une des méthodes d'installation décrites dans *Éléments à prendre en compte pour le déploiement à la page 4-10*.

Migration depuis des serveurs ServerProtect Normal

L'outil ServerProtect™ Normal Server Migration est un outil qui vous aide à faire migrer vers le client OfficeScan les ordinateurs exécutant Trend Micro ServerProtect Normal Server.

L'outil ServerProtect Normal Server Migration possède les mêmes spécifications logicielles et matérielles que le serveur OfficeScan. Exécutez l'outil sur des ordinateurs équipés de Windows Server 2003 ou Windows Server 2008.

Lorsque la désinstallation du serveur ServerProtect Normal est correctement exécutée, le client OfficeScan est installé. Celle-ci fait également migrer les paramètres de liste d'exclusion de scan (pour tous les types de scan) vers le client OfficeScan.

Pendant l'installation du client OfficeScan, le délai d'attente du programme d'installation client de l'outil de migration peut expirer, auquel cas le programme vous signale l'échec de l'installation. Toutefois, le client OfficeScan peut avoir été correctement installé. Vérifiez l'installation sur l'ordinateur client depuis OfficeScan Web Console.

La migration échoue dans les circonstances suivantes :

- Le client distant ne dispose que d'une adresse IPv6. L'outil de migration ne prend pas en charge l'adressage IPv6.
- Le client distant ne peut pas utiliser le protocole NetBIOS
- Les ports 455, 337 et 339 sont bloqués
- Le client distant ne peut pas utiliser le protocole RPC.

- Le service de registre distant est arrêté

Remarque

L'outil ServerProtect Normal Server Migration ne désinstalle pas l'agent Control Manager™ pour ServerProtect. Pour obtenir des instructions sur le mode de désinstallation de l'agent, consultez la documentation ServerProtect et/ou Control Manager.

Utilisation de l'outil ServerProtect Normal Server Migration

Tâche

1. Sur l'ordinateur du serveur OfficeScan, ouvrez le <*dossier d'installation du serveur*> `\PCCSRV\Admin\Utility\SPNSXfr` et copiez les fichiers `SPNSXfr.exe` et `SPNSX.ini` dans le `<dossier d'installation du serveur>\PCCSRV\Admin`.

2. Cliquez deux fois sur le fichier `SPNSXfr.exe` pour ouvrir l'outil.

   La console de l'outil **Server Protect Normal Server Migration** s'ouvre.

3. Sélectionnez le serveur OfficeScan. Le chemin du serveur OfficeScan s'affiche sous le chemin du serveur OfficeScan. S'il est incorrect, cliquez sur **Browse** et sélectionnez le dossier `PCCSRV` du répertoire dans lequel vous avez installé OfficeScan. Pour permettre à l'outil de retrouver automatiquement le serveur OfficeScan lors de la prochaine ouverture de l'outil, cochez la case **Détection automatique du chemin du serveur** (cochée par défaut).

4. Sélectionnez les ordinateurs exécutant ServerProtect Normal Server sur lesquels effectuer la migration en cliquant l'une des options suivantes sous **Target computer** :

   - **Arbre du réseau Windows** :affiche une arborescence des domaines du réseau. Pour sélectionner des ordinateurs à l'aide de cette méthode, cliquez sur les domaines dans lesquels rechercher des ordinateurs clients.

   - **Nom du serveur d'informations** : recherche par nom de serveur d'informations. Pour sélectionner des ordinateurs à l'aide de cette méthode, saisissez le nom d'un serveur d'informations sur le réseau dans la zone de texte. Pour rechercher plusieurs serveurs d'informations, insérez un point-virgule « ; » entre les noms de serveurs.

- **Nom précis du serveur habituel** : recherche par nom de Normal Server. Pour sélectionner des ordinateurs à l'aide de cette méthode, saisissez le nom d'un serveur Normal Server sur le réseau dans la zone de texte. Pour rechercher plusieurs serveurs habituels, saisissez un point-virgule (;) entre les noms de serveurs.
- **Recherche de la plage IP** : recherche par une plage d'adresses IP. Pour sélectionner des ordinateurs à l'aide de cette méthode, saisissez une plage d'adresses IP de classe B sous IP range.

Remarque

Si un serveur DNS sur le réseau ne répond pas lorsque vous recherchez des clients, la recherche est bloquée. Attendez l'expiration du délai de recherche.

5. Sélectionnez **Redémarrer après l'installation** pour redémarrer automatiquement les ordinateurs cibles après la migration.

   Il faut redémarrer les ordinateurs pour que la migration soit exécutée correctement. Si vous ne choisissez pas cette option, redémarrez manuellement les ordinateurs après la migration.

6. Cliquez sur **Rechercher**.

   Les résultats de la recherche s'affichent sous **ServerProtect Normal Servers**.

7. Cliquez sur les ordinateurs sur lesquels effectuer la migration.

   a. Pour sélectionner tous les ordinateurs, cliquez sur **Select All**.

   b. Pour désélectionner tous les ordinateurs, cliquez sur **Tout désélectionner**.

   c. Pour exporter la liste en tant que fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**.

8. Si la connexion sur les ordinateurs cibles requiert un nom d'utilisateur et un mot de passe, procédez comme suit :

   a. Cochez la case **Use group account/password**.

   b. Cliquez sur **Définir le compte de connexion**.

      L'écran Enter Administration Information s'affiche.

c. Saisissez le nom d'utilisateur et le mot de passe.

Remarque

Utilisez le compte administrateur local/domaine pour vous connecter à l'ordinateur cible. Si vous vous connectez avec des privilèges insuffisants, en tant qu'invité ou utilisateur normal par exemple, vous ne pourrez pas réaliser l'installation.

d. Cliquez sur **OK**.

e. Cliquez sur **Ask again if logon is unsuccessful** afin de pouvoir saisir de nouveau le nom d'utilisateur et le mot de passe durant le processus de migration si la connexion est impossible.

9. Cliquez sur **Migrate**.

10. Si vous n'avez pas sélectionné l'option **Redémarrer après l'installation** , redémarrez les ordinateurs pour compléter la migration.

Tâches après l'installation

Une fois l'installation effectuée, vérifiez les éléments suivants :

- *Raccourci du client OfficeScan à la page 4-68*
- *Liste des programmes à la page 4-68*
- *Services du client OfficeScan à la page 4-68*
- *Journaux d'installation du client OfficeScan à la page 4-69*

Raccourci du client OfficeScan

Les raccourcis du client OfficeScan apparaîssent dans le menu Démarrer de Windows sur l'ordintateur du client.

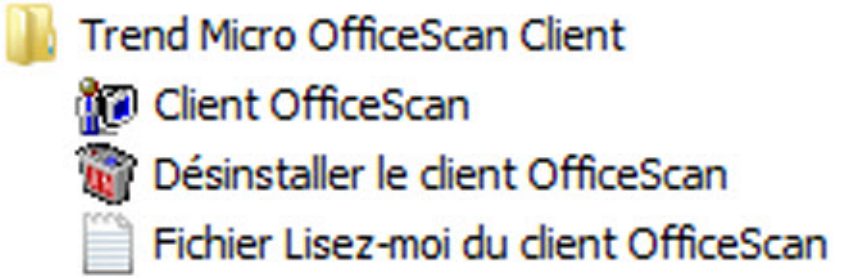


FIGURE 4-2. Raccourci du client OfficeScan

Liste des programmes

Client OfficeScan se trouve dans la liste **Ajout/Suppression de programmes** du Panneau de configuration de l'ordinateur client.

Services du client OfficeScan

Les services suivants du client OfficeScan s'affichent dans **Microsoft Management Console** :

- Service d'écoute d'OfficeScan NT (`TmListen.exe`)
- Service de scan en temps réel d'OfficeScanNT (`NTRtScan.exe`)
- Service proxy d'OfficeScan NT (`TmProxy.exe`)
- Pare-feu d'OfficeScan NT (`TmPfw.exe`), si le pare-feu a été activé durant l'installation

- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)

Journaux d'installation du client OfficeScan

Le journal d'installation du client OfficeScan, OFCNT.LOG, `se trouve` aux emplacements suivants :

- `%windir%` pour toutes les méthodes d'installation à l'exception de celle utilisant un pack MSI
- `%temp%` pour la méthode d'installation à l'aide du pack MSI

Tâches recommandées après l'installation

Trend Micro recommande d'effectuer les tâches suivantes après l'installation :

Mises à jour des composants

Mettez à jour les composants du client OfficeScan afin de garantir la protection la plus à jour des clients contre les risques de sécurité. Vous pouvez effectuer manuellement des mises à jour client depuis la console Web ou demander aux utilisateurs d'exécuter l'option « Mettre à jour » depuis leurs ordinateurs.

Tester OfficeScan à l'aide du script de test EICAR

L'EICAR (European Institute for Computer Antivirus Research), institut européen pour la recherche sur les antivirus informatiques, a mis au point un script de test permettant de confirmer l'installation et la configuration appropriées du logiciel antivirus. Pour plus d'informations, consultez le site Web de l'EICAR :

http://www.eicar.org

Le script de test de l'EICAR est un fichier texte inerte qui porte l'extension `.com`. Il ne s'agit pas d'un virus et il ne contient aucun fragment de code viral mais la plupart des logiciels antivirus réagissent à sa présence comme s'il s'agissait d'un virus. Utilisez ce fichier pour simuler un incident viral et vérifier que les notifications par e-mail et les journaux de virus fonctionnent correctement.

AVERTISSEMENT!

N'utilisez jamais de véritables virus pour tester votre produit antivirus.

Exécution d'un test de scan

Tâche

1. Activez le scan en temps réel sur l'ordinateur client.
2. Copiez la chaîne de caractères suivante et collez-la dans un éditeur de texte tel que le Bloc-notes : `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Enregistrez le fichier sous le nom `EICAR.com` dans un répertoire temporaire. OfficeScan détecte immédiatement le fichier.
4. Pour tester d'autres ordinateurs du réseau, joignez le fichier EICAR.com à un e-mail et envoyez-le à l'un des ordinateurs.

Conseil

Trend Micro vous recommande de compresser le fichier EICAR à l'aide d'un logiciel de compression tel que WinZip, puis d'effectuer un autre scan de test.

Désintallation du client OfficeScan

Il existe deux façons de désinstaller le client OfficeScan à partir des ordinateurs :

- *Désinstallation du client OfficeScan de la console Web à la page 4-71*
- *Exécution du programme de désinstallation du client OfficeScan à la page 4-73*

Si le client OfficeScan dispose d'une installation du Cisco Trust Agent (CTA), la désinstallation du programme client OfficeScan peut entraîner ou non la suppression de l'agent. Cela dépend des paramètres que vous avez configurés lors du déploiement de l'agent. Pour plus d'informations, voir *Déploiement de Cisco Trust Agent à la page 15-30*.

Si Cisco Trust Agent est présent après que vous avez installé le client OfficeScan, supprimez-le manuellement de l'écran à partir de l'écran **Ajout/Suppression de programmes**.

Si vous ne parvenez pas à désinstaller le client OfficeScan à l'aide des méthodes ci-dessus, désinstallez-le manuellement. Pour obtenir des informations détaillées, voir *Désinstallation manuelle du client OfficeScan. à la page 4-73*.

Désinstallation du client OfficeScan de la console Web

Désinstallez le programme client OfficeScan à partir de la console Web N'effectuez la désinstallation que si vous rencontrez des problèmes avec le programme. Procédez à la réinstallation immédiatement pour continuer à protéger l'ordinateur contre les risques de sécurité.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Tâches** > **Désinstallation du client**.
4. Sur l'écran **Désinstallation du client**, cliquez sur **lancer la désinstallation**. Le serveur envoie une notification aux clients.
5. Vérifiez l'état de notification et assurez-vous que tous les clients ont reçu une notification.
   a. Cliquez sur **Sélectionner les ordinateurs non informés**, puis sur **Lancer la désinstallation** pour envoyer immédiatement une nouvelle notification aux clients non informés.
   b. Cliquez sur **Arrêter la désinstallation** pour qu'OfficeScan arrête d'envoyer des notifications aux clients recevant actuellement des notifications. Les clients déjà informés et effectuant déjà la désinstallation ignorent cette commande.

Le programme de désinstallation du client OfficeScan

Accordez aux utilisateurs le droit de désinstaller le programme du client OfficeScan, puis demandez-leur d'exécuter le programme de désinstallation du client depuis leur ordinateur.

Selon votre configuration, la désinstallation peut nécessiter un mot de passe. Si c'est le cas, veillez à partager le mot de passe uniquement avec les utilisateurs qui exécuteront le programme de désinstallation et à le modifier immédiatement s'il a été divulgué à d'autres utilisateurs.

Autorisation du privilège de désinstallation du client OfficeScan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Désinstallation**.
5. Pour autoriser la désinstallation sans mot de passe, sélectionnez **Autoriser l'utilisateur à désinstaller le client OfficeScan**. Si un mot de passe est nécessaire, sélectionnez **Demander un mot de passe à l'utilisateur lors de la désinstallation du client OfficeScan**, entrez un mot de passe et confirmez-le.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Exécution du programme de désinstallation du client OfficeScan

Tâche

1. Dans le menu **Démarrer** de Windows, cliquez sur **Programmes** > **Trend Micro OfficeScan Client** > **Désinstaller le client OfficeScan**.

   Vous pouvez également effectuer cette procédure :

   a. Cliquez **Panneau de configuration** > **Ajout/Suppression de programmes**.

   b. Sélectionnez **Trend Micro OfficeScan Client** et cliquez sur **Modifier**.

   c. Suivez les instructions à l'écran.

2. Si vous y êtes invité, entrez le mot de passe de désinstallation. OfficeScan informe l'utilisateur sur la progression de la désinstallation et l'avertit lorsque celle-ci est terminée. L'utilisateur ne doit pas redémarrer l'ordinateur client pour terminer la désinstallation.

Désinstallation manuelle du client OfficeScan.

Procédez à la désinstallation manuelle uniquement si vous rencontrez des problèmes pour désinstaller le client OfficeScan à partir de la console Web ou après avoir exécuté le programme de désinstallation.

Tâche

1. Connectez-vous à l'ordinateur à l'aide d'un compte disposant de privilèges d'administrateur.

2. Cliquez avec le bouton droit de la souris sur l'icône du client OfficeScan dans la barre d'état système et sélectionnez **Décharger OfficeScan**. Si vous êtes invité à saisir un mot de passe, indiquez le mot de passe de déchargement, puis cliquez sur Ok.

Remarque

Désactivez le mot de passe sur les ordinateurs sur lesquels le client OfficeScan le client sera déchargé. Pour obtenir des informations détaillées, voir *Configuration des privilèges clients et autres paramètres à la page 13-90*.

3. Si vous n'avez pas spécifié le mot de passe de déchargement, arrêtez les services suivants depuis Microsoft Management Console :
   - Service d'écoute d'OfficeScan NT
   - Pare-feu d'OfficeScan NT
   - Service de scan en temps réel d'OfficeScanNT
   - Service proxy d'OfficeScan NT
   - Service de prévention des modifications non autorisées
4. Cliquez sur **Démarrer** > **Programmes**, cliquez avec le bouton droit de la souris sur **Trend Micro OfficeScan Client** et cliquez sur **Supprimer**.
5. Ouvrez l'éditeur de la base de registre (`regedit.exe`).

AVERTISSEMENT!

Cette procédure implique que vous supprimiez les clés de registre. Le fait d'apporter des modifications erronées à votre base de registre peut gravement affecter votre système. Effectuez toujours une copie sauvegarde avant de procéder à toute modification de la base de registre. Consultez l'aide de l'Éditeur du Registre pour obtenir des informations complémentaires.

6. Supprimez les clés de registre suivantes d'OfficeScan :
   - Si aucun autre produit Trend Micro n'est installé sur l'ordinateur :
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

       Pour les ordinateurs 64 bits :

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`
   - Si d'autres produits Trend Micro sont installés sur l'ordinateur, supprimez uniquement les clés suivantes :

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog

  Pour les ordinateurs 64 bits :

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp

  Pour les ordinateurs 64 bits :

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\PC-cillinNTCorp

7. Supprimez les clés/valeurs de registre suivantes :

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
- Moniteur OfficeScanNT (REG_SZ) sous HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

8. Supprimez toutes les instances des clés de registre suivantes aux emplacements ci-après :

- Emplacements :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
  - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services
  - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services
- Clés :
  - NTRtScan
  - tmcfw
  - tmcomm

- TmFilter
- TmListen
- tmpfw
- TmPreFilter
- TmProxy
- tmtdi
- VSApiNt
- tmlwf (pour les ordinateurs Windows Vista / Windows Server 2008 / 7)
- tmwfp (pour les ordinateurs Windows Vista / Windows Server 2008 / 7)
- tmactmon
- TMBMServer
- tmevtmgr

9. Fermez l'Éditeur du Registre.
10. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** et double-cliquez sur **Système**.
11. Cliquez sur l'onglet **Matériel**, puis sur **Gestionnaire de périphériques**.
12. Cliquez sur **Affichage** > **Afficher les périphériques cachés**.
13. Développez **Pilotes non-Plug and Play** et désinstallez les périphériques suivants :
    - tmcomm
    - tmactmon
    - tmevtmgr
    - Filtre Trend Micro
    - Préfiltre Trend Micro
    - Pilote TDI Trend Micro

- Trend Micro VSAPI NT
- Service de prévention des modifications non autorisées
- Pilote d'appel externe WFP Trend Micro (pour les ordinateurs Windows Vista / Windows Server 2008 / 7)

14. Désinstallez le pilote du pare-feu commun.

a. Cliquez avec le bouton droit de la souris sur **Emplacements de mon réseau** et cliquez sur **Propriétés**.

b. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** et cliquez sur **Propriétés**.

c. Dans l'onglet **Général**, sélectionnez **Pilote du pare-feu commun Trend Micro** et cliquez sur **Désinstaller**.

Remarque

Les étapes suivantes s'appliquent uniquement sur les systèmes d'exploitation Windows Vista/Server 2008/7. Les clients utilisant tous les systèmes d'exploitation passent à l'étape 15.

d. Cliquez avec le bouton droit de la souris sur **Réseau** et cliquez sur **Propriétés**.

e. Cliquez sur **Gérer les connexions réseau**.

f. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** et cliquez sur **Propriétés**.

g. Dans l'onglet **Réseau**, sélectionnez **Trend Micro NDIS 6.0 Filter Driver** et cliquez sur **Désinstaller**.

15. Redémarrez l'ordinateur client.

16. Si aucun autre produit Trend Micro n'est installé sur l'ordinateur, supprimez le répertoire d'installation `Trend Micro` (généralement `C:\Program Files \Trend Micro`). Pour les ordinateurs 64 bits, le dossier d'installation figure sous `C:\Program Files (x86)\Trend Micro`.

17. Si d'autres produits Trend Micro sont installés, supprimez les dossiers suivants :

- <*Dossier d'installation du client*>
- Le dossier `BM` sous le dossier d'installation Trend Micro (généralement, `C:\Program Files\Trend Micro\BM` pour les systèmes 32 bits et `C:\Program Files (x86)\Trend Micro\BM` pour les systèmes 64 bits)

Chapitre 5

Maintien d'une protection à jour

Ce chapitre décrit les composants de OfficeScan™Trend Micro™ et les procédures de mise à jour.

Sujets abordés dans ce chapitre:

- *Composants et programmes OfficeScan à la page 5-2*
- *Présentation de la mise à jour à la page 5-12*
- *Mises à jour du serveur OfficeScan à la page 5-15*
- *Mises à jour du serveur Smart Protection Server intégré à la page 5-27*
- *Mise à jour des clients OfficeScan à la page 5-27*
- *Agents de mise à jour à la page 5-55*
- *Résumé des mises à jour de composants à la page 5-64*

Composants et programmes OfficeScan

OfficeScan utilise des composants et des programmes pour protéger les ordinateurs clients contre les derniers risques de sécurité. Tenez ces composants et ces programmes à jour en exécutant des mises à jour manuelles ou programmées.

Outre les composants, les clients OfficeScan reçoivent également des fichiers de configuration mis à jour du serveur OfficeScan. Les clients ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. À chaque fois que vous modifiez les paramètres d'OfficeScan via la console Web, les fichiers de configuration sont modifiés.

Les composants sont regroupés de la façon suivante :

- *Composants de l'antivirus à la page 5-2*
- *Composants de Damage Cleanup Services à la page 5-6*
- *Composants du service Anti-spyware à la page 5-6*
- *Composants du pare-feu à la page 5-7*
- *Composant lié à la réputation de sites Web à la page 5-8*
- *Composants de surveillance des comportements à la page 5-8*
- *Programmes à la page 5-9*

Composants de l'antivirus

Les composants d'antivirus comprennent les signatures, les pilotes et les moteurs suivants :

- *Fichiers de signatures de virus à la page 5-3*
- *Moteur de scan antivirus à la page 5-4*
- *Pilote de scan antivirus à la page 5-5*
- *Signatures IntelliTrap à la page 5-6*

- *Signatures d'exceptions IntelliTrap à la page 5-6*

Fichiers de signatures de virus

Le fichier de signatures de virus disponible sur un ordinateur client dépend de la méthode de scan utilisée par le client. Pour plus d'informations sur les méthodes de scan, voir *Méthodes de scan à la page 6-8*.

TABLEAU 5-1. Fichiers de signatures de virus

MÉTHODE DE SCAN	FICHIER DE SIGNATURES UTILISÉ
Scan traditionnel	Le **Fichier de signatures de virus** contient des informations qui aident OfficeScan à identifier les virus ainsi que les les programmes malveillants d'attaques mixtes les plus récents. Trend Micro crée et publie de nouvelles versions du fichier de signatures de virus plusieurs fois par semaine et chaque fois qu'un virus/programme malveillant particulièrement ravageur est détecté. Trend Micro vous conseille de programmer les mises à jour automatiques au moins toutes les heures. Cette fréquence est configurée par défaut sur tous les produits livrés.

MÉTHODE DE SCAN	FICHIER DE SIGNATURES UTILISÉ
Smart Scan	En mode Smart Scan, les clients OfficeScan utilisent deux fichiers de signatures légers qui fonctionnent ensemble pour protéger de la même façon que les fichiers de signatures anti-programmes malveillants et anti-spyware conventionnels. Une source Smart Protection héberge le **Smart Scan Pattern** (fichier de signatures Smart Scan). Ce fichier de signatures est mis à jour toutes les heures et contient la majorité des définitions de signatures. Les clients Smart scan ne téléchargent pas ce fichier de signatures. Les clients vérifient les menaces potentielles par rapport au fichier de signatures en envoyant des requêtes de scan à la source Smart Protection. La source de mise à jour du client (serveur OfficeScan ou source de mise à jour personnalisée) héberge le **Smart Scan Agent Pattern**. Ce fichier de signatures est mis à jour quotidiennement et contient toutes les autres définitions de signatures introuvables dans le Smart Scan Pattern. Les clients téléchargent ce fichier de signatures à partir de la source de mise à jour en utilisant la même méthode que pour le téléchargement des composants OfficeScan. Pour plus d'informations sur les fichiers Smart Scan Pattern et Smart Scan Agent Pattern, voir *Fichiers de signatures Smart Protection à la page 3-8*.

Moteur de scan antivirus

Au cœur de tous les produits Trend Micro se trouve le moteur de scan, initialement conçu en réponse aux premiers virus de fichiers. Le moteur de scan actuel est exceptionnellement sophistiqué et capable de détecter différents types de *Virus et programmes malveillants à la page 6-2*. Le moteur de scan détecte également les virus sous contrôle conçus et utilisés pour la recherche.

Plutôt que de scanner chaque octet de chaque fichier, le moteur et le fichier de signatures collaborent à l'identification des éléments suivants :

- Caractéristiques révélatrices du code du virus
- Emplacement précis dans un fichier dans lequel se trouve le virus

OfficeScan supprime les virus/programmes malveillants détectés et restaure l'intégrité du fichier.

Mise à jour du moteur de scan

Grâce à l'enregistrement des informations de virus/programmes malveillants à durée de vie critique dans le fichier de signatures de virus, Trend Micro minimise le nombre de mises à jour du moteur de scan, tout en maintenant la protection à jour. Néanmoins, Trend Micro met régulièrement à disposition de nouvelles versions du moteur de scan. Trend Micro fournit de nouveaux moteurs dans les circonstances suivantes :

- Intégration de nouvelles technologies de scan et de détection au logiciel
- Découverte d'un nouveau virus/programme malveillant potentiellement dangereux que le moteur de scan n'est pas capable de traiter
- Optimisation des performances du scan
- Ajout de formats de fichiers, de langages de script, de formats de chiffrement et/ou de compression

Pilote de scan antivirus

Le pilote de scan antivirus contrôle les opérations de l'utilisateur sur les fichiers. Ces opérations incluent l'ouverture ou la fermeture des fichiers, ainsi que l'exécution d'une application. Il existe deux versions pour ce pilote. Il s'agit de `TmXPFlt.sys` et `TmPreFlt.sys`. `TmXPFlt.sys` est utilisé pour la configuration en temps réel du moteur de scan antivirus et `TmPreFlt.sys` pour le contrôle des opérations de l'utilisateur.

Remarque

Ce composant ne s'affiche pas sur la console. Pour vérifier la version, accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Pccnt\Drv`. Cliquez avec le bouton droit de la souris sur le fichier `.sys`, sélectionnez **Propriétés** et accédez à l'onglet **Version**.

Signatures IntelliTrap

La signature IntelliTrap (pour plus de détails, voir *IntelliTrap à la page C-7*). La signature détecte en temps réel les fichiers compressés en fichiers exécutables.

Signatures d'exceptions IntelliTrap

Le fichier de signatures d'exceptions IntelliTrap contient une liste des fichiers de compression « approuvés »

Composants de Damage Cleanup Services

Les composants Damage Cleanup Services se composent du moteur et du modèle suivants.

- *Moteur de nettoyage de virus à la page 5-6*
- *Modèle de nettoyage de virus à la page 5-6*

Moteur de nettoyage de virus

Le Moteur de nettoyage de virus recherche et supprime les chevaux de Troie et leurs processus. Ce moteur est compatible avec les plates-formes 32 et 64 bits.

Modèle de nettoyage de virus

Le Modèle de nettoyage de virus est utilisé par le Moteur de nettoyage de virus pour identifier les fichiers et processus infestés de chevaux de Troie afin de les éliminer.

Composants du service Anti-spyware

Les composants anti-spyware conprennent le moteur et les signatures suivants :

- *Signatures de spywares à la page 5-7*
- *Moteur de scan anti-spyware à la page 5-7*
- *Signatures de surveillance active des spywares à la page 5-7*

Signatures de spywares

Le Fichier de signatures de spywares identifie les spywares/graywares dans les fichiers et les programmes, les modules dans la mémoire, la base de registre de Windows et les raccourcis d'URL.

Moteur de scan anti-spyware

Le Moteur de scan anti-spyware recherche les spywares et les graywares, puis effectue l'action de scan appropriée. Ce moteur est compatible avec les plates-formes 32 et 64 bits.

Signatures de surveillance active des spywares

La signature de surveillance active des spywares est utilisée pour l'analyse anti-spyware et anti grayware en temps réel. Seuls les clients de scan traditionnel utilisent ce fichier de signatures.

Les clients Smart scan utilisent le Smart Scan Agent Pattern (fichier de signatures de l'agent Smart Scan) pour le scan anti-spyware et anti-grayware en temps réel. Les clients envoient des requêtes de scan à une source Smart Protection si le risque de la cible du scan ne peut pas être déterminé pendant le scan.

Composants du pare-feu

Les composants de pare-feu se composent du pilote et du fichier de signatures suivants :

- *Pilote du pare-feu commun à la page 5-7*
- *Signatures du pare-feu commun à la page 5-8*

Pilote du pare-feu commun

Le Pilote de pare-feu commun est utilisé avec le fichier de signatures du pare-feu commun pour rechercher des virus réseau sur les ordinateurs clients. Ce pilote est compatible avec les plates-formes 32 et 64 bits.

Signatures du pare-feu commun

Tout comme le fichier de signatures de virus, le fichier de signatures du pare-feu commun aide OfficeScan à identifier les signatures de virus, signatures uniques des bits et des octets qui signalent la présence d'un virus de réseau.

Composant lié à la réputation de sites Web

Le composant lié à la réputation des sites Web est le Moteur de filtre URL.

Moteur de filtre URL

Le Moteur de filtre URL facilite la communication entre OfficeScan et le service de filtre d'URL de Trend Micro. Le service de filtre d'URL est un système qui évalue les URL et fournit des informations d'évaluation à OfficeScan.

Composants de surveillance des comportements

Les composants de surveillance des comportements se composent des signatures, pilotes et services suivants :

- *Signatures de détection de l'analyse comportementale à la page 5-8*
- *Pilote de surveillance des comportements à la page 5-9*
- *Service principal de surveillance des comportements à la page 5-9*
- *Modèle de configuration de la surveillance des comportements à la page 5-9*
- *Digital Signature Pattern à la page 5-9*
- *Modèle de conformité aux stratégies à la page 5-9*

Signatures de détection de l'analyse comportementale

Ce fichier de signatures contient les règles de détection des comportements de menaces suspects.

Pilote de surveillance des comportements

Ce pilote de noyau contrôle les événements système et les transmet au Service principal de surveillance des comportements pour l'application des stratégies.

Service principal de surveillance des comportements

Ce service en mode utilisateur offre les fonctions suivantes :

- Détection des rootkits
- Régulation de l'accès aux périphériques externes
- Protection des fichiers, des clés de registres et des services

Modèle de configuration de la surveillance des comportements

Le Pilote de la surveillance des comportements utilise ce fichier de signatures pour identifier les événements système normaux et les exclure de l'application des stratégies.

Digital Signature Pattern

Ce fichier de signatures contient la liste de signatures numériques valides utilisées par le Service principal de surveillance des comportements afin de déterminer si un programme responsable d'un événement système ne présente pas de danger.

Modèle de conformité aux stratégies

Le Service principal de surveillance des comportements vérifie les événements système et les compare aux stratégies de ce fichier de signatures.

Programmes

OfficeScan utilise les programmes et mises à jour des produits suivants :

- *Programme client OfficeScan à la page 5-10*
- *Cisco Trust Agent à la page 5-10*
- *Correctifs de type hotfix, patchs et Service Packs à la page 5-10*

Programme client OfficeScan

Le programme client OfficeScan assure la protection effective contre les risques de sécurité

Cisco Trust Agent

Cisco Trust Agent active la communication entre le client et les routeurs qui prennent en charge Cisco NAC. Cet agent ne fonctionne que si vous installez Policy Server for Cisco NAC.

Correctifs de type hotfix, patchs et Service Packs

Après la publication officielle d'un produit, Trend Micro développe souvent les éléments suivants afin de corriger les problèmes, d'améliorer les performances des produits ou d'y ajouter de nouvelles fonctionnalités.

- *Correctif de type hotfix à la page C-5*
- *Patch à la page C-10*
- *Correctif de sécurité à la page C-12*
- *Service Pack à la page C-12*

Votre revendeur ou votre service d'assistance technique peut vous contacter lorsque ces éléments sont disponibles. Consultez le site Web de Trend Micro pour obtenir des informations sur les nouveaux correctifs de type hotfix, patchs et service packs :

http://www.trendmicro.com/download/emea/?lng=fr

Toutes les versions incluent un fichier Lisez-moi contenant des informations relatives à l'installation, au déploiement et à la configuration. Veuillez lire attentivement le fichier Lisez-moi avant d'exécuter l'installation.

Historique des correctifs de type hotfix et des patchs

Lorsque le serveur OfficeScan déploie des fichiers de correctifs de type hot fix ou de patchs sur les clients OfficeScan, le programme client enregistre des informations les concernant dans l'éditeur de registre. Vous pouvez lancer des requêtes sur ces informations pour plusieurs clients en utilisant des logiciels de logistique tels que Microsoft SMS, LANDesk™ ou BigFix™.

Remarque

Cette fonction n'enregistre pas les correctifs de type hot fix et les patchs qui ne sont déployés que sur le serveur.

Cette fonction est disponible à partir d'OfficeScan 8.0 Service Pack 1 avec le correctif 3,1.

- Les clients ayant effectué la mise à niveau de la version 8.0 Service Pack 1 à l'aide du correctif 3.1 ou ultérieur doivent enregistrer les correctifs de type hot fix et les patchs installés pour les versions 8.0 et ultérieures.
- Les clients ayant effectué la mise à niveau à partir des versions antérieures à la version 8.0 Service Pack 1 avec le correctif 3.1 enregistrent les correctifs de type hot fix et les correctifs installés pour les versions 10.0 et ultérieures.

Les informations sont stockées dans les clés suivantes :

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- Pour les ordinateurs exécutant les plates-formes x64 :

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

Recherchez les clés suivantes :

- **Clé** : `HotFix_installed`

  Type : `REG_SZ`

  Valeur : `<Nom du correctif de type hotfix ou du patch>`

- **Clé** : `HotfixInstalledNum`

  Type : `DWORD`

  Valeur : `<Numéro du correctif de type hotfix ou du patch>`

Présentation de la mise à jour

Toutes les mises à jour des composants proviennent du serveur Trend Micro ActiveUpdate Server. Lorsque des mises à jour sont disponibles, le serveur OfficeScan et les sources Smart Protection (Smart Protection Server ou Smart Protection Network) téléchargent les composants à jour. Il n'y a aucun risque de chevauchement de téléchargement de composants car les serveur OfficeScan et les sources Smart Protection téléchargent chacun un ensemble de composants spécifiques.

Remarque

Vous pouvez configurer le serveur OfficeScan et le serveur Smart Protection Server pour effectuer la mise à jour à partir d'une autre source que le serveur Trend Micro ActiveUpdate Server. Pour ce faire, vous devez définir une source de mise à jour personnalisée. Si vous avez besoin d'aide pour définir cette source de mise à jour, contactez votre service d'assistance.

Mise à jour du serveur OfficeScan et client OfficeScan

Le serveur OfficeScan télécharge la plupart des composants dont le client a besoin. Le seul composant qu'il ne télécharge pas est le fichier Smart Scan Pattern, qui est téléchargé par les sources Smart Protection.

Si un serveur OfficeScan gère un grand nombre de clients, la mise à jour peut utiliser une quantité significative de ressources du serveur, ce qui nuit à la stabilité et aux performances de ce dernier. Pour résoudre ce problème, OfficeScan possède une fonction d'agent de mise à jour qui permet de répartir sur certains clients la tâche de distribution des mises à jour vers les autres clients.

Le tableau suivant décrit les différentes options de mise à jour des composants pour le serveur et les clients OfficeScan Server, ainsi que les recommandations d'utilisation :

TABLEAU 5-2. Options de mise à jour serveur-client

OPTION DE MISE À JOUR	DESCRIPTION	RECOMMANDATION
Serveur ActiveUpdate > **Serveur** > **Client**	Le serveur OfficeScan reçoit les composants mis à jour à partir du serveur Trend Micro ActiveUpdate (ou d'une autre source de mise à jour) et lance la mise à jour des composants sur les clients.	Utilisez cette méthode s'il n'existe aucune section à faible bande passante entre les clients et le serveur OfficeScan.
Serveur ActiveUpdate > **Serveur** > **Agents de mise à jour** > **Client**	Le serveur OfficeScan reçoit les composants mis à jour à partir du serveur ActiveUpdate (ou d'une autre source de mise à jour) et lance la mise à jour des composants sur les clients. Les clients agissant en tant qu'agent de mise à jour demandent ensuite aux clients de mettre à jour les composants.	Si votre réseau comporte des sections à faible bande passante situées entre les clients et le serveur OfficeScan, utilisez cette méthode pour équilibrer le volume du trafic sur le réseau.
Serveur ActiveUpdate > **Agents de mise à jour** > **Client**	Les agents de mise à jour reçoivent les composants mis à jour directement à partir du serveur ActiveUpdate (ou d'une autre source de mise à jour) et demandent aux clients de mettre à jour les composants.	Utilisez cette méthode uniquement si vous rencontrez des difficultés pour mettre à jour les agents de mise à jour à partir du serveur OfficeScan ou des autres agents de mise à jour. Dans la majorité des cas, les agents de mise à jour reçoivent les mises à jour plus rapidement à partir du serveur OfficeScan ou des autres agents de mise à jour qu'à partir d'une source de mise à jour externe.

OPTION DE MISE À JOUR	DESCRIPTION	RECOMMANDATION
Serveur ActiveUpdate > Client	Les clients OfficeScan reçoivent les composants mis à jour directement depuis le serveur ActiveUpdate (ou depuis une autre source de mise à jour).	Utilisez cette méthode uniquement si vous rencontrez des difficultés pour mettre à jour les clients à partir du serveur OfficeScan ou des agents de mise à jour. Dans la majorité des cas, les clients reçoivent les mises à jour plus rapidement à partir du serveur OfficeScan ou des agents de mise à jour qu'à partir d'une source de mise à jour externe.

Mise à jour des sources Smart Protection

Une source Smart Protection (Smart Protection Server ou Smart Protection Network) télécharge le Smart Scan Pattern. Les clients Smart scan ne téléchargent pas ce fichier de signatures. Les clients vérifient les menaces potentielles par rapport au fichier de signatures en envoyant des requêtes de scan à la source Smart Protection.

Remarque

Consultez la rubrique *Sources Smart Protection à la page 3-6* pour obtenir de plus amples informations sur les sources Smart Protection.

Le tableau suivant décrit le processus de mise à jour pour les sources Smart Protection.

TABLEAU 5-3. Processus de mise à jour des sources Smart Protection

PROCESSUS DE MISE À JOUR	DESCRIPTION
Serveur ActiveUpdate > Smart Protection Network	Trend Micro Smart Protection Network reçoit les mises à jour du serveur Trend Micro ActiveUpdate Server. Les clients Smart scan qui ne sont pas connectés au réseau d'entreprise envoient des requêtes à Trend Micro Smart Protection Network.

Processus de mise à jour	Description
Serveur ActiveUpdate > **Smart Protection Server**	Un serveur Smart Protection Server (intégré ou autonome) reçoit les mises à jour du serveur Trend Micro ActiveUpdate. Les clients de Smart Protection qui sont connectés au réseau d'entreprise envoient des requêtes au serveur Smart Protection Server.
Smart Protection Network > **Smart Protection Server**	Un serveur Smart Protection Server (intégré ou autonome) reçoit les mises à jour de Trend Micro Smart Protection Network. Les clients de Smart Protection qui sont connectés au réseau d'entreprise envoient des requêtes au serveur Smart Protection Server.

Mises à jour du serveur OfficeScan

Le serveur OfficeScan télécharge les composants suivants et les déploie vers les clients:

Tableau 5-4. Composants téléchargés par le serveur OfficeScan

Composant	Distribution	
	Clients de scan traditionnel	Clients Smart Scan
Smart Scan Agent Pattern	Non	Oui
Fichier de signatures de virus	Oui	Non
Moteur de scan antivirus	Oui	Oui
Pilote de scan antivirus	Oui	Oui
Signatures IntelliTrap	Oui	Oui
Signatures d'exceptions IntelliTrap	Oui	Oui
Moteur de nettoyage de virus	Oui	Oui
Modèle de nettoyage de virus	Oui	Oui

COMPOSANT	DISTRIBUTION	
	CLIENTS DE SCAN TRADITIONNEL	CLIENTS SMART SCAN
Signatures de spywares	Oui	Oui
Moteur de scan anti-spyware	Oui	Oui
Signatures de surveillance active des spywares	Oui	Non
Pilote du pare-feu commun	Oui	Oui
Signatures du pare-feu commun	Oui	Oui
Moteur de filtre URL	Oui	Oui
Pilote de surveillance des comportements	Oui	Oui
Service principal de surveillance des comportements	Oui	Oui
Modèle de configuration de la surveillance des comportements	Oui	Oui
Signatures de détection de l'analyse comportementale	Oui	Oui
Digital Signature Pattern	Oui	Oui
Modèle de conformité aux stratégies	Oui	Oui

Rappels de mise à jour et conseils :

- Pour permettre au serveur de déployer les composants mis à jour sur les clients, activez la mise à jour automatique des clients. Pour obtenir des informations détaillées, voir *Mises à jour automatiques des clients OfficeScan à la page 5-37*. Si la mise à jour automatique des clients est désactivée, le serveur télécharge les mises à jour mais ne les déploie pas sur les clients.
- Un serveur OfficeScan IPv6 pur ne peut distribuer des mises à jour directement à des clients IPv4 purs. De même, un serveur OfficeScan IPv4 pur ne peut distribuer des mises à jour directement à des clients IPv6 purs. Un serveur proxy double pile

pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur OfficeScan de distribuer une mise à jour aux clients.

- Trend Micro publie des fichiers de signatures régulièrement pour maintenir à jour la protection des clients. De nouveaux fichiers de mise à jour étant régulièrement mis à disposition, OfficeScan utilise un mécanisme appelé **duplication des composants** permettant une mise à jour plus rapide des fichiers de signatures. Voir la *Duplication des composants du serveur OfficeScan à la page 5-20* pour plus d'informations.
- Si vous utilisez un serveur proxy pour vous connecter à Internet, utilisez les paramètres proxy corrects pour réussir le téléchargement des mises à jour.
- Sur le tableau de bord récapitulatif de la console Web, ajoutez le widget **Mises à jour du client** pour afficher les versions actuelles des composants et déterminer le nombre de clients ayant des composants à jour et obsolètes.

Sources de mise à jour du serveur OfficeScan

Configurez le serveur Smart Protection Server pour qu'il télécharge Smart Scan Pattern à partir du serveur Trend Micro ActiveUpdate ou d'une autre source. Vous pouvez indiquer une autre source si le serveur OfficeScan est incapable d'accéder directement au serveur ActiveUpdate. Pour un exemple de scénario, voir *Mises à jour de serveur OfficeScan isolé à la page 5-23*.

Une fois les mises à jour disponibles téléchargées par le serveur, il peut automatiquement envoyer une notification aux clients pour qu'ils mettent à jour leurs composants en fonction des paramètres spécifiés dans **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**. Si la mise à jour des composants est critique, laissez le serveur envoyer immédiatement une notification aux clients en accédant à **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour manuelle**.

Remarque

Si vous ne spécifiez pas de programme de déploiement, ni de paramètres de mises à jour déclenchées par un événement dans **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**, le serveur téléchargera les mises à jour mais n'enverra pas de notification aux clients pour qu'ils procèdent à la mise à jour.

Prise en charge d'IPv6 pour les mises à jour du serveur OfficeScan

Un serveur OfficeScan IPv6 pur ne peut effectuer directement de mises à jour à partir de sources de mise à jour IPv4 pures, telles que :

- Trend Micro ActiveUpdate Server
- Control Manager 5.5
- Control Manager 5.0

Remarque

L'adressage IPv6 est pris en charge pour Control Manager à partir de la version 5.5 SP1.

- Toute source de mise à jour personnalisée IPv4 pure

De même, un serveur OfficeScan IPv4 pur ne peut effectuer directement de mises à jour à partir de sources de mise à jour personnalisées IPv6 pures.

Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur de se connecter aux sources de mises à jour.

Proxy pour les mises à jour du serveur OfficeScan

Configurez les programmes du serveur hébergés sur l'ordinateur du serveur pour utiliser les paramètres proxy lors du téléchargement des mises à jour à partir du serveur Trend Micro ActiveUpdate. Les programmes du serveur incluent le serveur OfficeScan et le serveur Smart Protection Server intégré.

Configuration des paramètres proxy

Tâche

1. Accédez à **Administration** > **Paramètres proxy**.
2. Cliquez sur l'onglet **Proxy externe**.
3. Rendez-vous à la section **Mises à jour de l'ordinateur du serveur OfficeScan**.

4. Sélectionnez **Utiliser un serveur proxy pour les mises à jour de licence, de moteur ou de fichier de signatures**.

5. Indiquez le protocole de proxy, le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.

6. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

7. Cliquez sur **Enregistrer**.

Configuration de la source de mise à jour du serveur

Tâche

1. Accédez à **Mises à jour** > **Serveur** > **Source de mise à jour**.

2. Sélectionnez l'emplacement depuis lequel vous souhaitez télécharger les mises à jour de composants.

   Si vous choisissez le serveur ActiveUpdate, assurez-vous qu'il dispose d'une connexion Internet et, si vous utilisez un serveur proxy, testez si la connexion Internet peut être établie en utilisant les paramètres du proxy. Pour obtenir des informations détaillées, voir *Proxy pour les mises à jour du serveur OfficeScan à la page 5-18*.

   Si vous choisissez une source de mise à jour personnalisée, définissez l'environnement approprié et mettez à jour les ressources de cette source de mise à jour. Assurez-vous également qu'il existe une connexion opérationnelle entre le serveur et cette source de mise à jour. Si vous avez besoin d'aide pour définir une source de mise à jour, contactez votre service d'assistance.

   Remarque

   Le serveur OfficeScan utilise la duplication de composants lors du téléchargement des composants depuis la source de mise à jour. Voir *Duplication des composants du serveur OfficeScan à la page 5-20* pour obtenir des informations détaillées.

3. Cliquez sur **Enregistrer**.

Duplication des composants du serveur OfficeScan

Lorsque la dernière version d'un fichier de signatures complet est disponible au téléchargement sur le serveur Trend Micro ActiveUpdate server, 14 « fichiers de signatures incrémentiels » deviennent également disponibles. Les fichiers de signatures incrémentiels constituent des versions moins volumineuses que le fichier de signatures complet et correspondent à la différence entre la version la plus récente et la version précédente du fichier de signatures complet. Par exemple, si la version la plus récente est la version 175, le fichier de signatures incrémentiel v_173.175 contient les signatures de la version 175 absentes de la version 173 (la version 173 est la version précédente du fichier de signatures complet, puisque les numéros des fichiers de signatures sont déterminés par incrémentation de 2). Le fichier de signatures incrémentiel v_171.175 contient les signatures de la version 175 absentes de la version 171.

Pour réduire le trafic réseau généré lors du téléchargement du fichier de signatures le plus récent, OfficeScan effectue une duplication des composants, une méthode de mise à jour par laquelle le serveur OfficeScan ou l'agent de mise à jour télécharge uniquement les fichiers de signatures incrémentiels. Voir *Duplication des composants d'un agent de mise à jour à la page 5-62* pour plus d'informations sur la manière dont les agents de mise à jour dupliquent les composants.

La duplication des composants s'applique aux composants suivant :

- Fichier de signatures de virus
- Smart Scan Agent Pattern
- Modèle de nettoyage de virus
- Signatures d'exceptions IntelliTrap
- Signatures de spywares
- Signatures de surveillance active des spywares

Scénario de duplication des composants

Pour comprendre le processus de duplication des composants pour le serveur, reportez-vous au scénario suivant :

TABLEAU 5-5. Scénario de duplication des composants du serveur

Fichiers de signatures complets sur le serveur OfficeScan	Version actuelle : 171 Autres versions disponibles : 169	167	165	161	159	
Dernière version sur le serveur ActiveUpdate	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. Le serveur OfficeScan compare la version actuelle de son fichier de signatures complet avec la dernière version disponible sur le serveur ActiveUpdate. Si la différence entre les deux versions est inférieure ou égale à 14, le serveur ne télécharge que le fichier de signatures incrémentiel qui correspond à la différence entre les deux versions.

   Remarque

   si la différence est supérieure à 14, le serveur télécharge automatiquement la version complète du fichier de signatures et 14 fichiers de signatures incrémentiels.

   Voici un exemple :

   - La différence entre les versions 171 et 175 est de 2. En d'autres termes, le serveur ne dispose pas des versions 173 et 175.
   - Le serveur télécharge les fichiers de signatures incrémentiels 171.175. Le fichier de signatures incrémentiel correspond à la différence entre les versions 171 et 175.

2. Le serveur fusionne le fichier de signatures incrémentiel avec son fichier de signatures complet actuel pour générer le fichier de signatures complet le plus récent.

Voici un exemple :

- Sur le serveur, OfficeScan fusionne la version 171 avec le fichier de signatures incrémentiel 171.175 pour générer la version 175.
- Le serveur dispose d'un fichier de signatures incrémentiel (171.175) et du fichier de signatures complet le plus récent (version 175).

3. Le serveur génère des fichiers de signatures incrémentiels en fonction des autres fichiers de signatures complets disponibles sur le serveur. Si le serveur ne génère pas ces fichiers de signatures incrémentiels, les clients qui n'ont pas téléchargé les fichiers de signatures incrémentiels précédents procèdent automatiquement au téléchargement du fichier de signatures complet, ce qui entraîne une augmentation du trafic réseau.

   Voici un exemple :

   - Le serveur dispose des versions 169, 167, 165, 163, 161 et 159. Il peut donc générer les fichiers de signatures incrémentiels suivants :

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175
   - Dans la mesure où le serveur dispose déjà du fichier de signatures incrémentiel 171.175, il n'a pas besoin d'utiliser la version 171.
   - Le serveur dispose maintenant de 7 fichiers de signatures incrémentiels :

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175
   - Le serveur conserve les 7 derniers fichiers de signatures complets (versions 175, 171, 169, 167, 165, 163, 161). Il supprime toute version antérieure (version 159).

4. Le serveur compare ses fichiers de signatures incrémentiels actuels avec ceux disponibles sur le serveur ActiveUpdate. Le serveur télécharge les fichiers de signatures incrémentiels dont il ne dispose pas.

   Voici un exemple :

   - Le serveur ActiveUpdate dispose de 14 fichiers de signatures incrémentiels :

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- Le serveur OfficeScan dispose de 7 fichiers de signatures incrémentiels :

  171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- Le serveur OfficeScan procède au téléchargement de 7 fichiers de signatures incrémentiels supplémentaires :

  173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- Le serveur dispose maintenant de tous les fichiers de signatures incrémentiels disponibles sur le serveur ActiveUpdate.

5. Le fichier de signatures complet et les 14 fichiers de signatures incrémentiels sont mis à la disposition des clients.

Mises à jour de serveur OfficeScan isolé

Si le serveur OfficeScan appartient à un réseau qui est totalement isolé de l'ensemble des sources externes, vous pouvez maintenir les composants du serveur à jour en autorisant ce dernier à se mettre à jour depuis une source interne contenant les derniers composants.

Cette rubrique explique les tâches que vous devrez réaliser afin de mettre à jour un serveur OfficeScan isolé.

Mise à jour d'un serveur OfficeScan isolé

Cette procédure est fournie à titre informatif. Si vous êtes en mesure de réaliser toutes les tâches de cette procédure, veuillez contacter votre fournisseur d'accès pour obtenir des informations détaillées concernant chaque tâche de la procédure.

Tâche

1. Identifiez la source de mise à jour, par exemple, Trend Micro Control Manager ou un ordinateur hôte choisi aléatoirement. La source de mise à jour doit comprendre les éléments suivants :

- Une connexion Internet fiable, pour qu'elle puisse télécharger les derniers composants à partir du serveur Trend Micro ActiveUpdate. Sans connexion Internet, la seule façon pour la source de mise à jour d'obtenir les derniers

composants est que vous récupériez les composants vous-même à partir de Trend Micro et que vous les copiez dans la source de mise à jour.

- Une connexion opérationnelle au serveur OfficeScan. Configurez les paramètres proxy si un serveur proxy se trouve entre le serveur OfficeScan et la source de mise à jour. Pour obtenir des informations détaillées, voir *Proxy pour les mises à jour du serveur OfficeScan à la page 5-18*.
- Suffisamment d'espace disque pour les composants téléchargés.

2. Faites pointer le serveur OfficeScan vers la nouvelle source de mise à jour. Pour obtenir des informations détaillées, voir *Sources de mise à jour du serveur OfficeScan à la page 5-17*.
3. Identifiez les composants déployés sur les clients par le serveur. Voir *Mise à jour des clients OfficeScan à la page 5-27* pour obtenir la liste des composants déployables.

Conseil

L'un des moyens permettant de déterminer si un composant est en cours de déploiement sur des clients consiste à accéder à l'écran **Résumé des mises à jour** de la console Web (**Mises à jour** > **Résumé**). Dans cet écran, le taux de mise à jour d'un composant en cours de déploiement est toujours supérieur à 0 %.

4. Déterminez à quelle fréquence télécharger les composants. Les fichiers de signatures sont régulièrement mis à jour (quotidiennement dans certains cas), il est donc recommandé de les mettre à jour régulièrement. Pour les moteurs de scan et les pilotes, vous pouvez demander à votre service d'assistance de vous avertir en cas de mise à jour critique.
5. Concernant la source de mise à jour :
   a. Connectez-vous au serveur ActiveUpdate. L'URL du serveur dépend de votre version d'OfficeScan.
   b. Téléchargez les éléments suivants :
      - Le fichier `server.ini`. Ce fichier contient des informations sur les composants les plus récents.
      - Les composants que vous avez identifiés à l'étape 3.

c. Enregistrez les éléments enregistrés dans un répertoire de la source de mise à jour.

6. Exécutez une mise à jour manuelle du serveur OfficeScan. Pour obtenir des informations détaillées, voir *Mise à jour manuelle du serveur OfficeScan à la page 5-25*.

7. Répétez les étapes 5 et 6 chaque fois que vous devez mettre à jour des composants.

Méthodes de mise à jour du serveur OfficeScan

Mettez à jour les composants du serveur OfficeScan manuellement ou en configurant un programme de mise à jour.

Pour permettre au serveur de déployer les composants mis à jour sur les clients, activez la mise à jour automatique des clients. Pour obtenir des informations détaillées, voir *Mises à jour automatiques des clients OfficeScan à la page 5-37*. Si la mise à jour automatique des clients est désactivée, le serveur télécharge les mises à jour mais ne les déploie pas sur les clients.

Les méthodes de mise à jour comprennent :

- **Mise à jour manuelle du serveur** : Lorsqu'une mise à jour est capitale, effectuez une mise à jour manuelle afin que le serveur puisse obtenir les mises à jour immédiatement. Voir *Mise à jour manuelle du serveur OfficeScan à la page 5-25* pour obtenir des informations détaillées.

- **Mise à jour programmée du serveur** : Le serveur OfficeScan se connecte à la source de mise à jour au jour et à l'heure programmés pour obtenir les composants les plus récents. Voir *Programmation de mises à jour du serveur OfficeScan à la page 5-26* pour obtenir des informations détaillées.

Mise à jour manuelle du serveur OfficeScan

Mettez à jour manuellement les composants sur le serveur OfficeScan après l'installation ou la mise à niveau du serveur OfficeScan et en cas d'épidémie.

Tâche

1. Commencez une mise à jour manuelle par :

- Accédez à **Mises à jour** > **Serveur** > **Mise à jour manuelle**.
- Cliquez sur **Mise à jour immédiate du serveur** dans le menu principal de la console Web.

2. Sélectionnez les composants à mettre à jour.
3. Cliquez sur **Mettre à jour**.

   Le serveur télécharge les composants mis à jour.

Programmation de mises à jour du serveur OfficeScan

Configurez le serveur OfficeScan afin de vérifier régulièrement sa source de mise à jour et de télécharger automatiquement les mises à jour disponibles. Comme les clients reçoivent normalement des mises à jour du serveur, l'utilisation de la mise à jour programmée est un moyen simple et efficace de garantir que la protection contre les risques de sécurité est mise à jour en permanence.

Tâche

1. Accédez à **Mises à jour** > **Serveur** > **Mise à jour programmée**.
2. Sélectionnez **Activer la mise à jour programmée du serveur OfficeScan**.
3. Sélectionnez les composants à mettre à jour.
4. Programmez les mises à jour.

   Pour des mises à jour quotidiennes, hebdomadaires et mensuelles, la période correspond au nombre d'heures pendant lesquelles OfficeScan exécute la mise à jour. OfficeScan procède à la mise à jour à tout moment pendant cette période.
5. Cliquez sur **Enregistrer**.

Journaux de mise à jour du serveur OfficeScan

Consultez les journaux de mise à jour du serveur pour déterminer s'il existe des problèmes de mise à jour de certains composants. Les journaux incluent les mises à jour de composants pour le serveur OfficeScan.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de mise à jour

Tâche

1. Accédez à **Journaux** > **Journaux de mise à jour du serveur**.
2. Consultez la colonne **Résultat** pour vérifiez si des composants n'ont pas été mis à jour.
3. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Mises à jour du serveur Smart Protection Server intégré

L'Integrated Smart Protection Server intégré Smart Protection Server télécharge deux composants, appelés le Smart Scan Pattern et la Liste de blocage de sites Web. Pour obtenir des informations sur ces composants et leur méthode de mise à jour, consultez la rubrique *Gestion du serveur Smart Protection Server intégré à la page 3-19*.

Mise à jour des clients OfficeScan

Pour garantir le maintien de la protection des clients contre les derniers risques de sécurité encourus, procédez à une mise à jour régulière des composants clients.

Avant de mettre à jour les clients, vérifiez que leur source de mise à jour (serveur OfficeScan ou une source de mise à jour personnalisée) possède les composants les plus récents. Voir *Mises à jour du serveur OfficeScan à la page 5-15* pour obtenir des informations sur la méthode de mise à jour du serveur OfficeScan.

Le tableau suivant répertorie tous les composants que les sources de mise à jour déploient sur les clients et les composants en cas d'utilisation d'une méthode de scan spécifique.

TABLEAU 5-6. Composants OfficeScan déployés sur les clients

COMPOSANT	DISTRIBUTION	
	CLIENTS DE SCAN TRADITIONNEL	CLIENTS SMART SCAN
Smart Scan Agent Pattern	Non	Oui
Fichier de signatures de virus	Oui	Non
Moteur de scan antivirus	Oui	Oui
Pilote de scan antivirus	Oui	Oui
Signatures IntelliTrap	Oui	Oui
Signatures d'exceptions IntelliTrap	Oui	Oui
Moteur de nettoyage de virus	Oui	Oui
Modèle de nettoyage de virus	Oui	Oui
Signatures de spywares	Oui	Oui
Moteur de scan anti-spyware	Oui	Oui
Signatures de surveillance active des spywares	Oui	Non
Pilote du pare-feu commun	Oui	Oui
Signatures du pare-feu commun	Oui	Oui
Moteur de filtre URL	Oui	Oui
Pilote de surveillance des comportements	Oui	Oui
Service principal de surveillance des comportements	Oui	Oui

Composant	Distribution	
	Clients de scan traditionnel	Clients Smart Scan
Modèle de configuration de la surveillance des comportements	Oui	Oui
Signatures de détection de l'analyse comportementale	Oui	Oui
Digital Signature Pattern	Oui	Oui
Modèle de conformité aux stratégies	Oui	Oui

Sources de mise à jour des clients OfficeScan

Les clients peuvent obtenir des mises à jour depuis la source de mise à jour standard (serveur OfficeScan) ou des composants spécifiques depuis des sources de mises à jour personnalisées, telles que le serveur Trend Micro ActiveUpdate. Pour obtenir des informations détaillées, voir *Source de mise à jour standard pour les clients OfficeScan à la page 5-30* et *Sources de mise à jour personnalisées pour les clients OfficeScan à la page 5-31*.

Prise en charge d'IPv6 pour les mises à jour de clients OfficeScan

Un client IPv6 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv4 pur, telles que :

- un serveur OfficeScan IPv4 pur
- un agent de mise à jour IPv4 pur
- Toute source de mise à jour personnalisée IPv4 pure
- Trend Micro ActiveUpdate Server

De même, un client IPv4 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv6 pur, telles qu'un serveur OfficeScan ou un agent de mise à jour IPv6 pur.

Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients de se connecter aux sources de mises à jour.

Source de mise à jour standard pour les clients OfficeScan

Le serveur OfficeScan est la source de mise à jour standard pour les clients.

Si le serveur OfficeScan est injoignable, les clients ne disposeront pas de source de sauvegarde et seront par conséquent obsolètes. Pour mettre à jour les clients qui ne peuvent pas se connecter au serveur OfficeScan, Trend Micro recommande Client Packager. Utilisez cet outil pour créer un pack avec les derniers composants disponibles sur le serveur, puis exécutez le pack sur les clients.

Remarque

L'adresse IP du client (IPv4 ou IPv6) détermine si la connexion au serveur OfficeScan peut être établie. Pour plus d'informations sur la prise en charge d'IPv6 pour les mises à jour de clients, voir *Prise en charge d'IPv6 pour les mises à jour de clients OfficeScan à la page 5-29*.

Configuration de la source standard de mise à jour des clients OfficeScan

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Source de mise à jour**.
2. Sélectionnez **Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)**.
3. Cliquez sur **Notifier tous les clients**.

Processus de mise à jour de client OfficeScan

Remarque

Cette rubrique explique le processus de mise à jour des clients OfficeScan. Le processus de mise à jour des agents de mise à jour est traité dans la section *Source de mise à jour standard pour les clients OfficeScan à la page 5-30*.

Si vous configurez les clients OfficeScan pour la mise à jour directe à partir du serveur OfficeScan, le processus de mise à jour s'effectue de la façon suivante :

1. Le client OfficeScan obtient les mises à jour à partir du serveur OfficeScan.
2. Si vous n'arrivez pas à mettre à jour à partir du serveur OfficeScan, le client OfficeScan essaie de se connecter directement au serveur Trend Micro ActiveUpdate si l'option **Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server** est active dans **Ordinateurs en réseau** > **Paramètres clients généraux**, cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**.

Remarque

Seuls les composants peuvent être mis à jour depuis le serveur ActiveUpdate. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur OfficeScan ou des agents de mise à jour. Vous pouvez accélérer le processus de mise à jour en configurant les clients OfficeScan pour qu'ils téléchargent uniquement des fichiers de signature à partir du serveur ActiveUpdate. Pour plus d'informations, voir *Serveur ActiveUpdate comme source de mise à jour du client OfficeScan à la page 5-36*.

Sources de mise à jour personnalisées pour les clients OfficeScan

Outre le serveur OfficeScan, les clients OfficeScan peuvent effectuer la mise à jour depuis des sources de mise à jour personnalisées. Les sources de mise à jour personnalisées aident à réduire le trafic de mise à jour des clients OfficeScan dirigé vers le serveur OfficeScan et permettent aux clients OfficeScan ne pouvant pas se connecter au serveur OfficeScan d'obtenir des mises à jour rapides. Spécifiez les sources de mise à jour personnalisées dans la Liste de sources de mise à jour personnalisées, qui peut accueillir jusqu'à 1024 sources de mise à jour.

Conseil

Trend Micro recommande de définir certains clients OfficeScan en tant qu'Agents de mise à jour et de les ajouter à la liste.

Configuration des sources de mise à jour personnalisées pour les clients OfficeScan

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Source de mise à jour**.
2. Sélectionnez **Sources de mise à jour personnalisées** et cliquez sur **Ajouter**.
3. Dans l'écran qui s'affiche, indiquez les adresses IP des clients. Vous pouvez entrer une plage d'adresses IPv4 et/ou un préfixe IPv6 et sa longueur.
4. Spécifiez la source de mise à jour. Vous pouvez sélectionner un agent de mise à jour si un tel agent a été affecté ou saisir l'URL d'une source spécifique.

Remarque

Assurez-vous que les clients OfficeScan peuvent se connecter à la source de mise à jour en utilisant leurs adresses IP. Par exemple, si vous avez indiqué une plage d'adresses IPv4, la source de mise à jour doit avoir une adresse IPv4. Si vous avez indiqué un préfixe IPv6 et une longueur, la source de mise à jour doit avoir une adresse IPv6. Pour plus d'informations sur la prise en charge d'IPv6 pour les mises à jour de clients, voir *Sources de mise à jour des clients OfficeScan à la page 5-29*.

5. Cliquez sur **Enregistrer**.
6. Exécutez des tâches diverses présentées à l'écran.

   a. Sélectionnez l'un des paramètres suivants. Pour plus de détails sur la gestion de ces paramètres, reportez-vous à *Processus de mise à jour de client OfficeScan à la page 5-30*.

   - **Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes clients et des correctifs de type hot fix uniquement à partir du serveur OfficeScan**
   - **Mettre à jour des composants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables**

- **Mettre à jour les paramètres de domaine à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables**
- **Mettre à jour les programmes clients et les correctifs de type hotfix à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables**

b. Si vous avez indiqué au moins un agent de mise à jour comme source, cliquez sur **Rapport d'analyse de l'agent de mise à jour** pour générer un rapport mettant en évidence l'état de la mise à jour des clients. Pour plus de détails sur ce rapport, voir *Rapport d'analyse de l'agent de mise à jour à la page 5-63*.

c. Modifiez une source de mise à jour en cliquant sur le lien Plage d'adresses IP. Modifiez les paramètres dans l'écran qui s'affiche puis cliquez sur **Enregistrer**.

d. Supprimez une source de mise à jour depuis la liste en cochant la case correspondante et en cliquant sur **Supprimer**.

e. Pour déplacer une source de mise à jour, cliquez sur la flèche haut ou bas. Vous ne pouvez déplacer qu'une source à la fois.

7. Cliquez sur **Notifier tous les clients**.

Processus de mise à jour de client OfficeScan

Remarque

Cette rubrique explique le processus de mise à jour des clients OfficeScan. Le processus de mise à jour des agents de mise à jour est traité dans la section *Sources de mises à jour personnalisées pour les agents de mises à jour à la page 5-59*.

Après avoir défini et enregistré la liste des sources de mise à jour personnalisées, le processus de mise à jour s'effectue de la façon suivante :

1. Un client OfficeScan effectue la mise à jour à partir de la première source de la liste.

2. S'il ne peut pas effectuer la mise à jour à partir de la première source, le client OfficeScan essaie avec la seconde source, et ainsi de suite.

3. S'il ne peut effectuer la mise à jour à partir d'aucune des sources, le client OfficeScan vérifie les paramètres suivants sur l'écran Source de mise à jour :

TABLEAU 5-7. Paramètres supplémentaires de sources de mise à jour personnalisées

PARAMÈTRE	DESCRIPTION
Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes clients et des correctifs de type hot fix uniquement à partir du serveur OfficeScan	Si ce paramètre est actif, les agents de mise à jour s'exécutent directement à partir du serveur OfficeScan et ignorent l'option Liste des sources de mise à jour personnalisées. Si ce paramètre est désactivé, les agents de mise à jour appliquent les paramètres personnalisés de source de mise à jour configurés pour des clients normaux.

PARAMÈTRE	DESCRIPTION
Les clients mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables : Composants	Si ce paramètre est activé, le client procède à la mise à jour des composants à partir du serveur OfficeScan. S'il est désactivé, le client essaie ensuite de se connecter directement au serveur Trend Micro ActiveUpdate si l'une des conditions suivantes est vérifiée : • Dans **Ordinateurs en réseau** > **Paramètres clients généraux**, cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server** est activée. • Le serveur ActiveUpdate n'est pas inclus dans la liste de sources de mise à jour personnalisées. **Remarque** Seuls les composants peuvent être mis à jour depuis le serveur ActiveUpdate. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur OfficeScan ou des agents de mise à jour. Vous pouvez accélérer le processus de mise à jour en configurant les clients pour qu'ils téléchargent uniquement des fichiers de signature à partir du serveur ActiveUpdate. Pour plus d'informations, voir *Serveur ActiveUpdate comme source de mise à jour du client OfficeScan à la page 5-36*.
Les clients mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables : Paramètres de domaine	Si ce paramètre est activé, le client met à jour les paramètres au niveau du domaine à partir du serveur OfficeScan.

PARAMÈTRE	DESCRIPTION
Les clients mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables : Programmes clients et correctifs de type hotfix	Si ce paramètre est activé, le client met à jour les programmes et les correctifs de type hotfix à partir du serveur OfficeScan.

4. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, le client abandonne le processus de mise à jour.

Serveur ActiveUpdate comme source de mise à jour du client OfficeScan

Lorsque les clients OfficeScan téléchargent des mises à jour directement depuis Trend Micro ActiveUpdate server, vous pouvez restreindre le téléchargement aux fichiers de signatures pour réduire la bande passante consommée pendant les mises à jour et accélérer le processus de mise à jour.

Les moteurs de scan et autres composants ne sont pas mis à jour aussi régulièrement que des fichiers de signatures, ce qui justifie là aussi le fait de restreindre le téléchargement aux fichiers de signatures uniquement.

Un client IPv6 pur ne peut pas directement faire une mise à jour à partir du serveur Trend Micro ActiveUpdate Server. Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients OfficeScan de se connecter au serveur ActiveUpdate.

Limitation des téléchargements à partir du serveur ActiveUpdate

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Accédez à la section **Mises à jour**.

3. Sélectionnez **Télécharger uniquement les fichiers de signatures du serveur ActiveUpdate lors de l'exécution des mises à jour**.

Méthodes de mise à jour du client OfficeScan

Les clients OfficeScan qui mettent à jour des composants à partir du serveur OfficeScan ou d'une source de mise à jour personnalisée peuvent utiliser les méthodes de mise à jour suivantes :

- **Mises à jour automatiques des clients :** La mise à jour du client s'exécute automatiquement soit lorsque certains événements se produisent ou soit en fonction d'une programmation. Pour obtenir des informations détaillées, voir *Mises à jour automatiques des clients OfficeScan à la page 5-37*.
- **Mises à jour manuelles des clients :** Lorsqu'une mise à jour est capitale, effectuez une mise à jour manuelle pour demander immédiatement aux clients d'effectuer la mise à jour des composants. Pour obtenir des informations détaillées, voir *Mise à jour manuelle des clients OfficeScan à la page 5-44*.
- **Mises à jour en fonction des privilèges** : Les utilisateurs ayant des privilèges de mise à jour ont davantage de contrôle sur la manière dont le client OfficeScan est mis à jour sur leur ordinateur. Pour obtenir des informations détaillées, voir *Mettre à jour les privilèges et autres paramètres pour les clients OfficeScan à la page 5-46*.

Mises à jour automatiques des clients OfficeScan

La mise à jour automatique vous évite de demander à tous les clients d'effectuer une mise à jour et supprime tout risque de présence de composants obsolètes sur des ordinateurs clients.

Outre ces composants, les clients OfficeScan reçoivent également des fichiers de configuration mis à jour au cours de la mise à jour automatique. Les clients ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. À chaque fois que vous modifiez les paramètres d'OfficeScan via la console Web, les fichiers de configuration sont modifiés. Pour spécifier la fréquence à laquelle les fichiers de configuration sont appliqués aux clients, reportez-vous à l'étape 3 *Mise à jour automatique des composants du client OfficeScan à la page 5-40*.

Remarque

Vous pouvez configurer les clients pour qu'ils utilisent des paramètres proxy lors de la mise à jour automatique. Voir *Proxy pour la mise à jour des composants du client OfficeScan à la page 5-49* pour obtenir des informations détaillées.

Il existe deux types de mise à jour automatique :

- *Mises à jour déclenchées par un événement à la page 5-38*
- *Mises à jour programmées à la page 5-39*

Mises à jour déclenchées par un événement

Le serveur peut demander aux clients en ligne de mettre à jour les composants une fois le téléchargement des derniers composants effectué et informer les clients hors ligne lorsqu'ils redémarrent et se connectent au serveur. Vous pouvez aussi exécuter un scan immédiat (scan manuel) sur les ordinateurs clients OfficeScan après la mise à jour.

TABLEAU 5-8. Options de mise à jour déclenchée par un événement

OPTION	DESCRIPTION
Lancer la mise à jour des composants sur les clients immédiatement après le téléchargement d'un nouveau composant sur le serveur OfficeScan	Le serveur demande aux clients d'effectuer la mise à jour dès qu'il termine une mise à jour. Les clients mis à jour fréquemment ne doivent télécharger que des fichiers de signatures incrémentiels, ce qui réduit le temps nécessaire pour effectuer la mise à jour (voir *Duplication des composants du serveur OfficeScan à la page 5-20* pour plus d'informations sur les fichiers de signatures incrémentiels). Toutefois, la mise à jour fréquente peut nuire de façon importante aux performances du serveur, en particulier si un grand nombre de clients effectuent une mise à jour en même temps. Si vous souhaitez mettre à jour des clients en mode itinérant, sélectionnez l'option Inclure les clients itinérants et les clients hors ligne. Voir *Privilège des clients OfficeScan itinérants à la page 13-20* pour plus d'informations sur le mode itinérant.

OPTION	DESCRIPTION
Configurer les clients pour qu'ils lancent une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les clients itinérants sont exclus)	Un client ayant manqué une mise à jour télécharge immédiatement les composants lorsqu'il établit la connexion avec le serveur. Il se peut qu'un client rate une mise à jour s'il est hors ligne ou si l'ordinateur sur lequel il est installé ne fonctionne pas.
Exécuter un scan immédiat après la mise à jour (clients itinérants exclus)	Le serveur informe les clients d'effectuer un scan après une mise à jour déclenchée par un événement. Vous pouvez envisager d'activer cette option si une mise à jour particulière est une réponse à un risque de sécurité qui s'est déjà répandu sur le réseau.

Remarque

si le serveur OfficeScan ne réussit pas à envoyer une notification de mise à jour aux clients une fois le téléchargement des composants effectué, il renvoie automatiquement la notification passé un délai de 15 minutes. Le serveur envoie au maximum cinq notifications de mise à jour dans l'attente de la réponse du client. Si la cinquième tentative est toujours infructueuse, le serveur arrête l'envoi des notifications. Si vous sélectionnez l'option de mise à jour des composants lorsque les clients redémarrent et se connectent au serveur, la mise à jour des composants ne sera pas interrompue.

Mises à jour programmées

L'exécution de mises à jour programmées est un privilège. Vous devez d'abord sélectionner les clients OfficeScan qui disposeront de ce privilège, puis ces clients OfficeScan exécuteront les mises à jour selon le programme.

Remarque

Pour utiliser la mise à jour programmée avec le mécanisme de traduction d'adresse réseau (Network Address Translation), voir *Configuration des mises à jour programmées du client OfficeScan avec NAT à la page 5-42*.

Mise à jour automatique des composants du client OfficeScan

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**.
2. Sélectionnez les événements qui déclencheront la mise à jour des composants.
   - **Lancer la mise à jour des composants sur les clients immédiatement après le téléchargement d'un nouveau composant sur le serveur OfficeScan**
   - **Configurer les clients pour qu'ils lancent une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les clients itinérants sont exclus)**
   - **Exécuter un scan immédiat après la mise à jour (clients itinérants exclus)**
3. Indiquez à quelle fréquence les clients disposant du privilège de mise programmée devront effectuer la mise à jour programmée.
   - Si vous avez accordé à des clients le privilège de mise à jour programmée, passez à l'étape suivante.
   - Si vous n'avez pas accordé à des clients le privilège de mise à jour programmée, effectuez d'abord ce qui suit :

   a. Accédez à l'**Ordinateurs en réseau** > **Gestion des clients**.

   b. Dans l'arborescence des clients, sélectionnez les clients pour lesquels vous souhaitez disposer du privilège.

   c. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

      - Option n°1 : Dans l'onglet **Privilèges**, allez à la section **Privilèges de mise à jour des composants**. Vous verrez l'option **Activer la mise à jour programmée**.
      - Option n°2 : Dans l'onglet **Autres paramètres**, accédez à la section **Paramètres de mise à jour**. Vous verrez une autre option **Activer la mise à jour programmée**.

Remarque

Si vous voulez permettre aux utilisateurs clients d'activer ou de désactiver la mise à jour programmée sur la console du client OfficeScan, activez les options 1 et 2. Après avoir enregistré les paramètres, les mises à jour s'exécuteront sur l'ordinateur client conformément au programme. L'exécution des mises à jour programmées ne cesse que lorsqu'un utilisateur client clique avec le bouton droit de la souris sur l'icône du client OfficeScan dans la barre d'état système et sélectionne **Désactiver la mise à jour programmée**.

Si vous voulez que la mise à jour programmée s'exécute toujours et souhaitez empêcher les utilisateurs clients de la désactiver, activez l'option 1 et désactivez l'option 2.

d. Enregistrez les paramètres.

4. Configurez la programmation.

a. Si vous sélectionnez **Minute(s)** ou **Heure(s)**, vous avez la possibilité d'activer l'option **Mise à jour des configurations du client une seule fois par jour**. Si vous n'activez pas cette option, le client OfficeScan extrait les composants mis à jour et tout fichier de configuration disponible sur le serveur à l'intervalle spécifié. Si vous cochez cette option, OfficeScan ne met à jour que les composants à l'intervalle spécifié et les fichiers de configuration une fois par jour.

Conseil

Trend Micro met à jour fréquemment les composants ; cependant, les paramètres de configuration d'OfficeScan changent probablement moins fréquemment. La mise à jour des fichiers de configuration avec les composants nécessite plus de bande passante et augmente le temps nécessaire à OfficeScan pour terminer la mise à jour. C'est la raison pour laquelle, Trend Micro recommande de mettre à jour les configurations du client OfficeScan une seule fois par jour.

b. Si vous sélectionnez **Tous les jours** ou **Une fois par semaine**, indiquez l'heure de la mise à jour et l'intervalle de temps au cours duquel le serveur OfficeScan demandera aux clients de mettre à jour les composants. Par exemple, si l'heure de début a été définie à 12h00 et que l'intervalle de temps est de 2 heures, OfficeScan demande de façon aléatoire à tous les clients en

ligne de mettre à jour les composants entre 12h00 et 14h00. Ce paramètre permet d'éviter que tous les clients en ligne se connectent simultanément au serveur à l'heure spécifiée, réduisant de manière significative le trafic sur le serveur.

5. Cliquez sur **Enregistrer**.

Les clients hors ligne ne seront pas informés. Si un client hors ligne se reconnecte une fois le délai écoulé, il peut encore mettre à jour les composants s'il a sélectionné **Configurer les clients pour qu'ils lancent une mise à jour des composants lorsqu'ils redémarrent** sous **Mise à jour déclenchée par un événement**. Sinon, ils mettent à jour les composants au prochain horaire programmé ou si vous lancez une mise à jour manuelle.

Configuration des mises à jour programmées du client OfficeScan avec NAT

Les problèmes suivants peuvent se poser si le réseau local utilise NAT :

- Les clients OfficeScan apparaissent hors ligne sur la console Web.
- Le serveur OfficeScan n'est pas en mesure d'avertir les clients des mises à jour et des modifications de la configuration.

Contournez ces problèmes en déployant sur le client OfficeScan les composants et fichiers de configuration mis à jour issus du serveur à l'aide d'une mise à jour programmée comme décrit ci-dessous.

Tâche

- Avant d'installer le client OfficeScan sur les ordinateurs clients :

  a. Configurez la mise à jour client programmée dans la section **Mise à jour programmée** de **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**.

  b. Accordez aux clients le privilège d'activer la mise à jour programmée dans l'**Ordinateurs en réseau** > **Gestion des clients**, cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Privilèges** > **Privilèges de mise à jour des composants**.

- Si les clients OfficeScan existent déjà sur les ordinateurs clients :

  a. Accordez aux clients le privilège d'activer la mise à jour immédiate dans l'**Ordinateurs en réseau** > **Gestion des clients**, cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Privilèges** > **Privilèges de mise à jour des composants**.

  b. Indiquez aux utilisateurs de mettre à jour manuellement les composants sur l'ordinateur client (en cliquant avec le bouton droit de la souris sur l'icône OfficeScan de la barre d'état système, puis sur « Mettre à jour ») pour obtenir les paramètres de configuration mis à jour.

Lorsque des clients OfficeScan effectuent une mise à jour, ils reçoivent à la fois les composants et les fichiers de configuration mis à jour.

Utilisation de l'outil de programmation de la mise à jour du domaine

La programmation des mises à jour configurée dans les mises à jour automatiques de client concerne uniquement les clients disposant de privilèges de mise à jour programmée. Pour les autres clients, vous pouvez définir une programmation des mises à jour distincte. Pour cela, configurez une programmation par domaines d'arborescence client. Tous les clients appartenant à un même domaine seront soumis à la programmation.

Remarque

Il n'est pas possible de définir une programmation de mises à jour pour un client ou un sous-domaine spécifique. Tous les sous-domaines sont soumis à la programmation configurée pour leur domaine parent.

Tâche

1. Enregistrez les noms de domaines d'arborescences client et les programmations de mises à jour.
2. Accédez au <*Dossier d'installation du serveur à la page 6*>`\PCCSRV\Admin\Utility\DomainScheduledUpdate`.
3. Copiez les fichiers suivants dans `<Dossier d'installation du serveur>\PCCSRV`:

- `DomainSetting.ini`
- `dsu_convert.exe`

4. Ouvrez `DomainSetting.ini` à l'aide d'un éditeur de texte comme le Bloc-notes.
5. Indiquez un domaine d'arborescence client, puis configurez la programmation des mises à jour pour le domaine. Répétez cette étape pour ajouter d'autres domaines.

Remarque

Des instructions de configuration détaillées sont indiquées dans le fichier `.ini`.

6. Enregistrez le fichier `DomainSetting.ini`.
7. Ouvrez une invite de commande et accédez au répertoire du dossier `PCCSRV`.
8. Entrez la commande suivante, puis appuyez sur `Entrée`.

```
dsuconvert.exe DomainSetting.ini
```

9. Dans la console Web, accédez à **Ordinateurs en réseau** > **Gestion des clients**.
10. Cliquez sur **Enregistrer**.

Mise à jour manuelle des clients OfficeScan

Mettez à jour les composants clients OfficeScan manuellement lorsque les composants clients OfficeScan sont particulièrement obsolètes et à chaque fois qu'il ya une épidémie. Les composants clients OfficeScan deviennent particulièrement obsolètes lorsque le client OfficeScan n'est pas en mesure de mettre à jour les composants à partir de la source de mise à jour pendant une période prolongée.

Outre les mises à jour de composants, les clients OfficeScan reçoivent automatiquement des fichiers de configuration mis à jour lors d'une mise à jour manuelle. Les clients OfficeScan ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. À chaque fois que vous modifiez les paramètres d'OfficeScan via la console Web, les fichiers de configuration sont modifiés.

Remarque

Outre l'exécution des mises à jour manuelles, vous pouvez accorder aux utilisateurs le privilège d'exécuter les mises à jour manuelles (également appelé « Mises à jour immédiates » sur les ordinateurs clients OfficeScan). Pour obtenir des informations détaillées, voir *Mettre à jour les privilèges et autres paramètres pour les clients OfficeScan à la page 5-46*.

Mise à jour manuelle des clients OfficeScan

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour manuelle**.
2. Les composants actuellement disponibles sur le serveur OfficeScan et la date de dernière mise à jour de ces composants s'affichent en haut de l'écran. Assurez-vous que les composants sont à jour avant de demander aux clients d'effectuer une mise à jour.

   Remarque

   Mettez à jour manuellement les composants obsolètes sur le serveur. Voir *Mise à jour manuelle des clients OfficeScan à la page 5-44* pour obtenir des informations détaillées.

3. Pour mettre à jour uniquement les clients ayant des composants obsolètes :
   a. Cliquez sur **Sélectionner les clients dont les composants sont obsolètes**.
   b. (Facultatif) Sélectionnez **Inclure le(s) client(s) itinérant(s) et hors ligne** :
      - Pour mettre à jour les clients itinérants avec une connexion opérationnelle au serveur.
      - Pour mettre à jour les clients hors ligne lorsqu'ils deviennent en ligne.
   c. Cliquez sur **Lancer la mise à jour**.

   Remarque

   Le serveur recherche les clients dont les versions de composant sont antérieures à celles du serveur, puis demande à ces clients d'effectuer une mise à jour. Pour vérifier l'état de la notification, accédez à l'écran **Mises à jour** > **Résumé**.

4. Pour mettre à jour les clients de votre choix :

   a. Sélectionnez **Sélectionner manuellement les clients**.

   b. Cliquez sur **Sélectionner**.

   c. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

   d. Cliquez sur **Lancer la mise à jour des composants**.

Remarque

Le serveur commence à demander à chaque client de télécharger les composants mis à jour. Pour vérifier l'état de la notification, accédez à l'écran **Mises à jour** > **Résumé**.

Mettre à jour les privilèges et autres paramètres pour les clients OfficeScan

Accordez aux utilisateurs clients certains privilèges, tels que l'exécution de «Mettre à jour» et l'activation d'une mise à jour programmée.

Exécuter l'option « Mettre à jour »

Les utilisateurs disposant de ce privilège peuvent mettre à jour les composants à la demande en cliquant avec le bouton droit sur l'icône du client OfficeScan dans la barre d'état système et en sélectionnant **Mettre à jour**. Vous pouvez autoriser les utilisateurs clients à utiliser des paramètres proxy lors de l'exécution de l'option « Mettre à jour ». Voir *Privilèges de configuration proxy pour les clients à la page 13-52* pour obtenir des informations détaillées.

AVERTISSEMENT!

Des paramètres proxy configurés par l'utilisateur incorrects peuvent entraîner des problèmes de mise à jour. Soyez prudent lorsque vous autorisez les utilisateurs à configurer leurs propres paramètres proxy.

Activer la mise à jour programmée

Ce privilège permet aux clients d'activer et de désactiver la mise à jour programmée. Les utilisateurs disposant du privilège peuvent activer/désactiver la mise à jour programmée, mais ils ne peuvent pas configurer la programmation. Vous devez indiquer le programme dans la section **Mise à jour programmée** de **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**.

Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server

Lorsque les mises à jour sont lancées, les clients OfficeScan obtiennent d'abord les mises à jour depuis la source de mise à jour spécifiée dans l'écran **Mises à jour** > **Ordinateurs en réseau** > **Source de mise à jour**. Si la mise à jour échoue, les clients essaient de procéder à la mise à jour à partir du serveur OfficeScan. La sélection de cette option permet aux clients de tenter une mise à jour depuis le serveur Trend Micro ActiveUpdate si la mise à jour depuis le serveur OfficeScan échoue.

Un client IPv6 pur ne peut pas directement faire une mise à jour à partir du serveur Trend Micro ActiveUpdate Server. Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients de se connecter au serveur ActiveUpdate.

Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client ni déployer des correctifs de type hotfix

Cette option permet d'effectuer les mises à jour de composants, mais empêche le déploiement des correctifs de type hotfix et la mise à niveau des clients OfficeScan.

Si vous ne sélectionnez pas cette option, tous les clients se connectent simultanément au serveur pour procéder à la mise à niveau ou à l'installation d'un correctif de type hotfix. Les performances risquent alors d'être considérablement diminuées si vous disposez d'un nombre important de clients. Si vous sélectionnez cette option, prévoyez comment minimiser les conséquences d'une mise à niveau du client OfficeScan ou du déploiement d'un correctif de type hotfix sur le serveur, puis appliquez ce plan.

Accord de privilèges de mise à jour aux clients OfficeScan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de mise à jour des composants**.
5. Sélectionnez les options suivantes :
   - **Exécuter l'option « Mettre à jour »**
   - **Activer la mise à jour programmée**
6. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Paramètres de mise à jour**.
7. Sélectionnez les options suivantes :
   - **Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server**
   - **Activer la mise à jour programmée**
   - **Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client ni déployer des correctifs de type hotfix**
8. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Configuration de l'espace disque réservé pour les mises à jour clients OfficeScan

OfficeScan attribue une certaine quantité d'espace disque client pour les correctifs de type hotfix, les fichiers de signatures, les moteurs de scan et les mises à jour des programmes. Par défaut, OfficeScan réserve 60 Mo d'espace disque.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Accédez à la section **Espace disque réservé**.
3. Sélectionnez **Réserver __ Mo d'espace disque pour les mises à jour**.
4. Sélectionnez le volume d'espace disque.
5. Cliquez sur **Enregistrer**.

Proxy pour la mise à jour des composants du client OfficeScan

Les clients OfficeScan utilisent les paramètres proxy pendant la mise à jour automatique ou s'ils sont autorisés à exécuter l'option «Mettre à jour».

TABLEAU 5-9. Paramètres proxy utilisés pendant les mises à jour des composants du client OfficeScan

MÉTHODE DE MISE À JOUR	PARAMÈTRES PROXY UTILISÉS	UTILISATION
Mise à jour automatique du client	• Paramètres proxy automatiques. Pour obtenir des informations détaillées, voir *Paramètres proxy automatique pour le client OfficeScan à la page 13-53*. • Paramètres proxy interne. Pour obtenir des informations détaillées, voir *Proxy interne pour les clients OfficeScan à la page 13-50*.	1. Les clients OfficeScan utilisent en priorité les paramètres proxy automatiques pour la mise à jour des composants. 2. Si les paramètres proxy automatiques ne sont pas activés, les paramètres proxy interne sont utilisés. 3. Si les deux sont désactivés, les clients n'utilisent pas de paramètres proxy.

MÉTHODE DE MISE À JOUR	PARAMÈTRES PROXY UTILISÉS	UTILISATION
Mettre à jour	• Paramètres proxy automatiques. Pour obtenir des informations détaillées, voir *Paramètres proxy automatique pour le client OfficeScan à la page 13-53*. • Paramètres proxy configurés par l'utilisateur. Vous pouvez accorder aux utilisateurs clients l'autorisation de configurer les paramètres proxy. Pour obtenir des informations détaillées, voir *Privilèges de configuration proxy pour les clients à la page 13-52*.	1. Les clients OfficeScan utilisent en priorité les paramètres proxy automatiques pour la mise à jour des composants. 2. Si les paramètres proxy automatiques ne sont pas activés, les paramètres proxy configurés par l'utilisateur sont utilisés. 3. Si les deux sont désactivés ou si les paramètres proxy automatiques sont désactivés alors que les utilisateurs clients ne disposent pas du privilège requis, les clients n'utilisent pas de proxy lors de la mise à jour des composants.

Configuration des notifications de mise à jour du client OfficeScan

OfficeScan notifie les utilisateurs clients lorsque des événements associés à la mise à jour se produisent.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Rendez-vous à la section **Paramètres d'alerte**.
3. Sélectionnez les options suivantes :
   - **Afficher l'icône d'alerte dans la barre des tâches Windows si le fichier de signatures de virus n'a pas été mis à jour au bout de __ jour(s)** : Une

icône d'alerte s'affiche dans la barre des tâches Windows pour rappeler aux utilisateurs de mettre à jour un fichier de signatures de virus n'ayant pas été mis à jour durant la période indiquée. Pour mettre à jour le fichier de signatures, utilisez l'une des méthodes de mise à jour indiquées dans *Méthodes de mise à jour du client OfficeScan à la page 5-37*.

Tous les clients gérés par le serveur appliqueront ce paramètre.

- **Afficher un message de notification si l'ordinateur client doit être redémarré pour charger un pilote de noyau** : Après l'installation d'un correctif de type hotfix ou d'un pack de mise à niveau qui contient une nouvelle version d'un pilote de noyau, la version précédente du pilote est susceptible d'être toujours présente sur l'ordinateur. Le seul moyen de décharger la version précédente et de charger la nouvelle est de redémarrer l'ordinateur. Une fois l'ordinateur redémarré, la nouvelle version est automatiquement installée et aucun redémarrage n'est nécessaire.

  Le message de notification s'affiche immédiatement après l'installation, par l'ordinateur client, du correctif de type hotfix ou du pack de mise à niveau.

4. Cliquez sur **Enregistrer**.

Affichage des journaux de mise à jour du client OfficeScan

Consultez les journaux de mise à jour du client pour déterminer s'il existe des problèmes de mise à jour du fichier de signatures de virus sur les clients.

Remarque

Dans cette version du produit, seuls les journaux de mise à jour des fichiers de signatures de virus peuvent être interrogés depuis la console Web.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Mise à jour des composants**.
2. Pour afficher le nombre de mises à jour des clients, cliquez sur **Afficher** dans la colonne **Progression**. L'écran **Progression de la mise à jour des composants** apparaît, il affiche le nombre de clients mis à jour toutes les 15 minutes, ainsi que le nombre total de clients mis à jour.
3. Pour afficher les clients qui ont mis à jour les fichiers de signatures de virus, cliquez sur **Afficher** dans la colonne **Détails**.
4. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Applicatios des mises à jour du client OfficeScan

Utilisez la conformité de la sécurité pour garantir que les clients disposent des derniers composants. La conformité de la sécurité détermine les incohérences des composants entre le serveur OfficeScan et les clients. Ces incohérences se produisent généralement lorsque les clients ne peuvent pas se connecter au serveur pour mettre à jour les composants. Si le client obtient une mise à jour d'une autre source (telle que le serveur ActiveUpdate), il est possible qu'un composant du client soit plus récent que celui du serveur.

Pour plus d'informations, voir *Conformité de la sécurité pour les clients gérés à la page 13-58*.

Rétrogadation des composants pour les clients OfficeScan

Rétrograder signifie revenir à une version précédente du fichier de signatures de virus, du fichier Smart Scan Agent Pattern et du moteur de scan antivirus. Si ces composants ne fonctionnent pas correctement, rétrogradez-les vers leur version précédente. OfficeScan conserve les versions actuelles et précédentes du moteur de scan antivirus et

les cinq dernières versions du fichier de signatures de virus et du fichier Smart Scan Agent Pattern.

Remarque

Seuls les composants mentionnés ci-dessus peuvent être rétrogradés.

OfficeScan utilise des moteurs de scan différents pour les clients exécutant des plates-formes 32 bits et 64 bits. Il est nécessaire de rétrograder ces moteurs de scan séparément. La procédure de rétrogradation est identique pour tous les types de moteurs.

Tâche

1. Accédez à **Mises à jour** > **Rétrograder**.
2. Cliquez sur **Synchroniser avec le serveur** dans la section appropriée.
   a. Dans l'arborescence des clients qui affichée, cliquez sur l'icône du domaine racine ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
   b. Cliquez sur **Rétrograder**.
   c. Cliquez sur **Afficher journaux de mise à jour** pour vérifier le résultat ou **Retour** pour revenir à l'écran Rétrograder.
3. Si une version antérieure du fichier de signatures existe sur le serveur, cliquez sur **Rétrograder les versions serveur et client** pour rétrograder le fichier de signature à la fois du client OfficeScan et du serveur.

Exécution de l'outil Touch Tool pour les correctifs de type Hot Fix des clients OfficeScan

L'outil Touch Tool synchronise l'horodatage d'un fichier grâce à celui d'un autre fichier ou de l'horloge système de l'ordinateur. Si vous ne parvenez pas à déployer un correctif de type hotfix sur le serveur OfficeScan, utilisez Touch Tool pour changer l'horodatage du correctif de type hotfix. OfficeScan considère alors qu'il s'agit d'un nouveau correctif de type hotfix, ce qui amène le serveur à tenter automatiquement un nouveau déploiement du correctif.

Tâche

1. Sur le serveur OfficeScan, accédez à <*Dossier d'installation du serveur*>>\PCCSRV\Admin\Utility\Touch.
2. Copiez le fichier `TMTouch.exe` dans le dossier contenant le fichier à modifier. Si vous synchronisez l'horodatage d'un fichier grâce à celui d'un autre fichier, placez les deux fichiers dans l'emplacement de l'outil Touch Tool.
3. Ouvrez une invite de commande et accédez à l'emplacement de l'outil Touch Tool.
4. Entrez ce qui suit :

   ```
   TmTouch.exe <nom fichier destination> <nom fichier source>
   ```

   Où :

   - `<nom fichier destination>` est le nom de fichier du correctif de type hotfix dont vous voulez changer l'horodatage
   - `<nom fichier source>` est le nom du fichier dont vous voulez répliquer l'horodatage

   Remarque

   Si vous ne définissez pas un nom de fichier source, l'outil définit l'horodatage du fichier de destination en fonction de l'heure du système de l'ordinateur. Utilisez le caractère générique (*) pour le fichier de destination, mais pas pour le nom du fichier source.

5. Pour vérifier que l'horodatage a bien été modifié, saisissez `dir` dans l'invite de commande ou vérifiez les propriétés du fichier dans l'Explorateur Windows.

Agents de mise à jour

Pour distribuer la tâche de déploiement des composants, des paramètres de domaine ou des programmes clients et des correctifs de type hotfix vers les clients OfficeScan, attribuez à certains clients OfficeScan le rôle d'agents de mise à jour, ou de sources de mise à jour pour les autres clients. Cela permet de s'assurer que les clients reçoivent des

mises à jour en temps et en heure, évitant au serveur OfficeScan d'avoir à gérer un trafic réseau trop important.

Si le réseau est segmenté par sites et si le lien réseau entre les segments présente un trafic élevé, affectez au moins un agent de mise à jour à chaque site.

Configuration minimale requise pour les agents de mise à jour

Visitez le site Web suivant pour obtenir la liste complète des configurations requises :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Configuration de l'agent de mise à jour

La configuration de l'agent de mise à jour s'effectue en 2 étapes:

1. Affectez un client OfficeScan en tant qu'agent de mise à jour à des composants spécifiques.
2. Spécifiez les clients qui seront mis à jour à partir de cet agent de mise à jour.

Remarque

Le nombre de connexions clients simultanées qu'un agent de mise à jour peut gérer dépend des spécifications matérielles de l'ordinateur.

Affectation d'un client OfficeScan en tant qu'agent de mise à jour

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, sélectionnez les clients qui seront désignés en tant qu'agents de mise à jour.

Remarque

Il n'est pas possible de sélectionner l'icône du domaine racine puisque tous les clients seraient alors désignés comme agents de mise à jour. Un agent de mise à jour IPv6 exclusif ne peut distribuer des mises à jour directement à des clients IPv4 exclusifs. De même, un agent de mise à jour IPv4 pur ne peut distribuer des mises à jour directement à des clients IPv6 purs. Un serveur proxy double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre à l'agent de mise à jour de distribuer des mises à jour aux clients.

3. Cliquez sur **Paramètres** > **Paramètres des agents de mise à jour**.
4. Sélectionnez les éléments que les agents de mise à jour peuvent partager.
   - Mises à jour des composants
   - Paramètres de domaine
   - Programmes clients et correctifs de type hotfix
5. Cliquez sur **Enregistrer**.

Spécification des clients OfficeScan qui seront mis à jour par un agent de mise à jour

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Source de mise à jour**.
2. Sous **Liste des sources de mise à jour personnalisées**, cliquez sur **Ajouter**.
3. Dans l'écran qui s'affiche, indiquez les adresses IP des clients. Vous pouvez entrer une plage d'adresses IPv4 et/ou un préfixe IPv6 et sa longueur.
4. Dans le champ **Agent de mise à jour**, sélectionnez l'agent de mise à jour que vous voulez attribuer aux clients.

Remarque

Assurez-vous que les clients peuvent se connecter à l'agent de mise à jour en utilisant leurs adresses IP. Par exemple, si vous avez spécifié une plage d'adresses IPv4, l'agent de mise à jour doit avoir une adresse IPv4. Si vous avez spécifié un préfixe IPv6 et une longueur de préfixe, l'agent de mise à jour doit comporter une adresse IPv6.

5. Cliquez sur **Enregistrer**.

Sources de mises à jour pour les agents de mises à jour

Les agents de mise à jour peuvent obtenir des mises à jour à partir de sources diverses, telles que le serveur OfficeScan ou à partir d'une source personnalisée. Configurez la source de mise à jour à partir de l'écran de source de mise à jour de la console Web.

Prise en charge d'IPv6 pour les agents de mise à jour

Un agent de mise à jour IPv6 pur ne peut effectuer directement de mises à jour à partir de sources de mise à jour IPv4 pures, telles que :

- un serveur OfficeScan IPv4 pur
- Toute source de mise à jour personnalisée IPv4 pure
- Trend Micro ActiveUpdate Server

De même, un agent de mise à jour IPv4 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv6 pur, telles qu'un serveur OfficeScan IPv6 pur.

Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents de mise à jour de se connecter aux sources de mise à jour.

Source de mise à jour standard pour les agents de mise à jour

Le serveur OfficeScan est la source de mise à jour standard pour les agents de mise à jour. Si vous configurez des agents pour la mise à jour directe à partir du serveur OfficeScan, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent de mise à jour obtient les mises à jour à partir du serveur OfficeScan.

2. S'il ne peut pas être mis à jour à partir du serveur OfficeScan, l'agent tente de se connecter directement à Trend Micro ActiveUpdate Server si l'une des conditions suivantes est remplie :

   - Dans **Ordinateurs en réseau** > **Paramètres clients généraux**, cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server** est activée.
   - Le serveur ActiveUpdate est la première entrée de la liste de sources de mise à jour personnalisées.

   Conseil

   Ne placez le serveur ActiveUpdate en haut de la liste que si vous rencontrez des problèmes de mise à jour à partir du serveur OfficeScan. Lorsque les agents de mise à jour effectuent la mise à jour directe à partir du serveur ActiveUpdate, ils consomment une portion significative de la bande passante réseau et Internet.

3. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Sources de mises à jour personnalisées pour les agents de mises à jour

En plus du serveur OfficeScan, les agents de mise à jour peuvent effectuer la mise à jour depuis des sources de mise à jour personnalisées. Les sources de mise à jour personnalisées aident à réduire le trafic de mise à jour du client dirigé vers le serveur OfficeScan. Spécifiez les sources de mise à jour personnalisées dans la Liste de sources de mise à jour personnalisées, qui peut accueillir jusqu'à 1024 sources de mise à jour. Voir *Sources de mise à jour personnalisées pour les clients OfficeScan à la page 5-31* pour connaître les étapes de configuration de la liste.

Remarque

Vérifiez que seuls les **agents de mise à jour, composants de mise à jour, paramètres de domaine et programmes client ainsi que les correctifs de type hot fix de l'option du serveur OfficeScan** sont désactivés sur

l'écran **Source de mise à jour (Ordinateurs en réseau)** (**Mises à jour** > **Ordinateurs en réseau** > **Source de mise à jour**) afin que les agents de mise à jour se connectent aux sources de mise à jour personnalisées.

Après avoir défini et enregistré la liste, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent de mise à jour effectue la mise à jour à partir de la première entrée de la liste.
2. S'il ne peut pas effectuer la mise à jour à partir de la première entrée, il essaie avec la seconde entrée, et ainsi de suite.
3. S'il ne peut effectuer la mise à jour à partir d'aucune des entrées, l'agent vérifie les options suivantes :

   - **Mettez à jour les composants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.

     Si l'option est désactivée, l'agent essaie ensuite de se connecter directement à Trend Micro ActiveUpdate Server si l'une des conditions suivantes est remplie :

     Remarque

     Vous ne pouvez mettre à jour des composants qu'à partir du serveur Active Update. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur ou des agents de mise à jour.

     - Dans l'**Ordinateurs en réseau** > **Gestion des clients**, cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server** est activée.
     - Le serveur ActiveUpdate n'est pas inclus dans la liste de sources de mise à jour personnalisées.

   - **Mettez les paramètres de domaine à jour à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.
   - **Mettez les programmes client et les correctifs de type hotfix à jour à partir du serveur OfficeScan si toutes les sources personnalisées sont**

indisponibles ou introuvables : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.

4. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Le processus de mise à jour est différent si l'option **Agent de mise à jour : toujours mettre à jour depuis la source de mise à jour standard (le serveur OfficeScan)** est activée et si le serveur OfficeScan notifie l'agent de mettre à jour les composants. Le processus est le suivant :

1. L'agent effectue la mise à jour directement à partir du serveur OfficeScan et ignore la liste des sources de mise à jour.
2. S'il ne peut pas être mis à jour à partir du serveur, l'agent tente de se connecter directement à Trend Micro ActiveUpdate Server si l'une des conditions suivantes est remplie :
   - Dans l'**Ordinateurs en réseau** > **Gestion des clients**, cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les clients téléchargent des mises à jour depuis Trend Micro ActiveUpdate Server** est activée.
   - Le serveur ActiveUpdate est la première entrée de la liste de sources de mise à jour personnalisées.

Conseil

Ne placez le serveur ActiveUpdate en haut de la liste que si vous rencontrez des problèmes de mise à jour à partir du serveur OfficeScan. Lorsque des clients OfficeScan effectuent la mise à jour directement depuis le serveur ActiveUpdate, ils consomment une portion significative de la bande passante réseau et Internet.

3. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Configuration de la source de mise à jour pour l'agent de mise à jour

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Source de mise à jour**.

2. Choisissez d'effectuer la mise à jour à partir de la source de mise à jour standard pour les agents de mise à jour (serveur OfficeScan) ou de la source de mise à jour personnalisée pour les agents de mise à jour.

3. Cliquez sur **Notifier tous les clients**.

Duplication des composants d'un agent de mise à jour

les agents de mise à jour utilisent la duplication des composants lors du téléchargement des composants, tout comme le fait le serveur OfficeScan. Voir *Duplication des composants du serveur OfficeScan à la page 5-20* pour plus d'informations sur la manière dont le serveur effectue la duplication des composants.

Le processus de duplication des composants pour les agents de mise à jour est le suivant :

1. L'agent de mise à jour compare la version actuelle de son fichier de signatures complet avec la dernière version disponible depuis la source de mise à jour. Si la différence entre les deux versions est inférieure ou égale à 14, l'agent de mise à jour ne télécharge que le fichier de signatures incrémentiel qui correspond à la différence entre les deux versions.

   Remarque

   Si la différence est supérieure à 14, l'agent de mise à jour télécharge automatiquement la version complète du fichier de signatures.

2. L'agent de mise à jour fusionne le fichier de signatures incrémentiel qu'il a téléchargé avec son fichier de signatures complet actuel pour générer le fichier de signatures complet le plus récent.

3. L'agent de mise à jour télécharge tous les fichiers de signatures incrémentiels restants depuis la source de mise à jour.

4. Le dernier fichier de signatures complet et tous les fichiers de signatures incrémentiels sont mis à la disposition des clients.

Méthodes de mise à jour pour les agents de mise à jour

Les agents de mise à jour utilisent des méthodes de mise à jour identiques à celles qu'utilisent les clients ordinaires. Pour obtenir des informations détaillées, voir *Méthodes de mise à jour du client OfficeScan à la page 5-37*.

Vous pouvez également utiliser l'outil de configuration des mises à jour programmées pour activer et configurer les mises à jour programmées sur un agent de mise à jour installé à l'aide de Client Packager.

Remarque

Cet outil n'est pas disponible si l'agent de mise à jour a été installé avec une autre méthode. Voir la *Éléments à prendre en compte pour le déploiement à la page 4-10* pour plus d'informations.

Utilisation de l'outil de configuration de mise à jour programmée

Tâche

1. Sur l'ordinateur de l'agent de mise à jour, accédez au <*dossier d'installation du client*>.
2. Double-cliquez sur le fichier `SUCTool.exe` pour exécuter l'outil. La console de l'outil de configuration des mises à jour programmées s'ouvre.
3. Sélectionnez **Activer la mise à jour programmée**.
4. Spécifiez la fréquence et l'heure de mise à jour.
5. Cliquez sur **Appliquer**.

Rapport d'analyse de l'agent de mise à jour

Générez le rapport d'analyse de l'agent de mise à jour pour analyser l'infrastructure de mise à jour et déterminer quels clients effectuent des téléchargements à partir du serveur OfficeScan, des agents de mise à jour ou du serveur Active Update. Ce rapport vous permet également de vérifier si le nombre de clients demandant des mises à jour à partir des sources de mise à jour dépasse les ressources disponibles, et de rediriger le trafic réseau vers les sources appropriées.

Remarque

Ce rapport englobe tous les agents de mise à jour. Si vous avez délégué la tâche de gestion d'un ou plusieurs domaines à d'autres administrateurs, ceux-ci visualisent également les agents de mise à jour appartenant aux domaines qu'ils ne gèrent pas.

OfficeScan exporte le Rapport d'analyse de l'agent de mise à jour dans un fichier de valeurs séparées par des virgules (`.CSV`).

Ce rapport contient les informations suivantes :

- Ordinateur client OfficeScan
- adresse IP
- Chemin de l'arborescence client
- Source de mise à jour
- Si les clients téléchargent ce qui suit à partir des agents de mise à jour :
  - Composants
  - Paramètres de domaine
  - Programmes client OfficeScan et correctifs de type hot fix

Pour plus de détails sur la génération du rapport, reportez-vous à *Sources de mise à jour personnalisées pour les clients OfficeScan à la page 5-31*.

Résumé des mises à jour de composants

La console Web comporte un écran **Résumé des mises à jour** (accédez à **Mises à jour** > **Résumé**) qui vous informe de l'état général des mises à jour des composants et vous permet de mettre à jour les composants obsolètes. Si vous activez la mise à jour programmée du serveur, l'écran affichera également la prochaine mise à jour programmée.

Actualisez périodiquement l'écran pour afficher l'état le plus récent de mise à jour des composants.

Remarque

Pour afficher les mises à jour des composants sur le Smart Protection Server intégré, accédez au **Smart Protection** > **Serveur intégré**.

État de mise à jour des clients OfficeScan

Si vous avez lancé la mise à jour des composants sur les clients, consultez les informations suivantes dans cette section:

- Nombre de clients informés de la mise à jour des composants à effectuer.
- Nombre de clients non informés mais déjà dans la file d'attente des notifications. Pour annuler la notification vers ces clients, cliquez sur **Annuler la notification**.

Composants

Dans le tableau **État de mise à jour**, vous pouvez afficher l'état de mise à jour de chaque composant que le serveur OfficeScan télécharge et distribue.

La version actuelle et la date de dernière mise à jour de chaque composant sont affichées. Cliquez sur le lien numéroté pour afficher les clients dont des composants sont obsolètes. Mettez à jour manuellement les clients dont des composants sont obsolètes.

Chapitre 6

Recherche des risques de sécurité

Ce chapitre explique comment protéger les ordinateurs des risques de sécurité en utilisant le scan de fichiers.

Sujets abordés dans ce chapitre :

- *À propos des risques de sécurité à la page 6-2*
- *Méthodes de scan à la page 6-8*
- *Types de scan à la page 6-14*
- *Paramètres communs à tous les types de scan à la page 6-27*
- *Privilèges et autres paramètres de scan à la page 6-52*
- *Paramètres de scan généraux à la page 6-69*
- *Journaux de risques de sécurité à la page 6-87*
- *Notifications sur les risques liés à la sécurité à la page 6-79*

À propos des risques de sécurité

« Risque de sécurité » est le terme générique regroupant les virus/programmes malveillants et les spywares/grayware. OfficeScan protège les ordinateurs contre les risques de sécurité en scannant les fichiers avant de mener une action spécifique selon chaque risque détecté. Un nombre élevé de risques de sécurité détectés en peu de temps témoigne d'une épidémie. OfficeScan OfficeScan peut aider à enrayer les épidémies en appliquant des stratégies de prévention des épidémies et en isolant les ordinateurs sur lesquels sont détectés les fichiers infectés jusqu'à ce qu'ils ne présentent plus aucun risque. Des notifications et des journaux vous aident à vous tenir informé des risques de sécurité tout en vous alertant lorsqu'une action immédiate s'impose.

Virus et programmes malveillants

Il existe des dizaines de milliers de virus/programmes malveillants et de nouveaux sont créés chaque jour. Alors qu'à une époque, ils étaient plus courants dans DOS ou Windows, les virus informatiques de notre époque peuvent provoquer des dommages importants en exploitant les failles de sécurité des réseaux d'entreprise, des systèmes de messagerie électronique et des sites Web.

- **Canular** : Programme similaire aux virus qui manipule souvent l'apparence des éléments affichés sur l'écran de l'ordinateur.
- **Virus/programmes malveillants probables** : Fichiers suspects ayant certaines des caractéristiques d'un virus/programme malveillant. Pour plus d'informations, consultez l'Encyclopédie des virus de Trend Micro :

  http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp
- **Rootkit** : Un programme (ou un ensemble de programmes) qui installe et exécute un code sur un système à l'insu de l'utilisateur et sans son autorisation. Il utilise une technique de camouflage pour maintenir une présence persistante et indétectable sur la machine. Les rootkits n'infectent pas les machines. Ils cherchent plutôt à fournir un environnement indétectable afin d'exécuter un code malveillant. Les rootkits sont installés sur les systèmes via un piratage psychologique, lors de l'exécution de programmes malveillants ou simplement en naviguant sur un site Web malveillant. Une fois installé, un pirate peut pratiquement effectuer n'importe quelle action sur le système, notamment l'accès à distance et l'espionnage. Il peut

également masquer des processus, des fichiers, des clés de registre et des canaux de communication.

- **Cheval de Troie** : Ce type de menace utilise souvent les ports pour accéder aux ordinateurs ou aux programmes exécutables. Les programmes Cheval de Troie ne se répliquent pas, mais résident dans des systèmes pour effectuer des opérations malveillantes, telles que l'ouverture des ports aux pirates. Les solutions antivirus conventionnelles peuvent détecter et supprimer les virus, mais pas les chevaux de Troie, notamment ceux qui ont déjà pénétré votre système.
- **Virus** : Programme qui se réplique. Pour ce faire, le virus doit s'attacher à d'autres fichiers programmes et s'exécuter chaque fois que le programme hôte est lancé.
    - **Code malicieux ActiveX** : Code résidant dans les pages Web qui exécutent des contrôles ActiveX™
    - **Virus du secteur d'amorçage** : Virus qui infecte le secteur d'amorçage d'une partition ou d'un disque.
    - **Virus infectant les fichiers COM et EXE** : Programme exécutable avec extensions `.com` ou `.exe`
    - **Code malveillant Java** : Virus indépendant du système d'exploitation écrit ou imbriqué dans Java™.
    - **Virus de macro** : Virus chiffré comme application macro qui est souvent inclus à un document.
    - **Virus réseau** : Un virus qui se répand sur le réseau n'est pas, à proprement parler, un virus de réseau. Seuls certains des types virus/programmes malveillants, comme les vers, peuvent être appelés virus de réseau. Plus spécifiquement, les virus de réseau utilisent les protocoles réseau tels que TCP, FTP, UDP, HTTP et les protocoles d'e-mail pour se multiplier. Souvent, ils n'affectent pas les fichiers système ou ne modifient pas les secteurs d'amorçage des disques durs. Par contre, les virus de réseau infectent la mémoire des ordinateurs clients en l'obligeant à inonder le réseau de trafic, ce qui peut entraîner des ralentissements, voire même une panne complète du réseau. Comme les virus de réseau restent en mémoire, ils sont souvent indétectables par les méthodes conventionnelles de scan de fichiers basées sur l'E/S.

Le pare-feu OfficeScan utilise le fichier de signatures du pare-feu commun pour identifier et bloquer les virus de réseau. Voir *À propos du pare-feu OfficeScan à la page 11-2* pour obtenir des informations détaillées.

- **Utilitaire de compression** : Programme exécutable compressé et/ou encodé Windows ou Linux™, souvent un cheval de Troie. La compression de fichiers exécutables rend l'utilitaire de compression plus difficile à détecter par les logiciels antivirus.
- **Virus de test** : Fichier inerte agissant comme un véritable virus et pouvant être détecté par les logiciels antivirus. Utilise des virus de test tels que le script de test EICAR afin de vérifier que le scan de votre installation antivirus fonctionne correctement.
- Virus **VBScript**, **JavaScript** ou **HTML** : Réside sur des pages Web et est téléchargé par un navigateur.
- **Vers** : Programme automatique ou ensemble de programmes qui peut répandre des copies fonctionnelles de lui-même ou de ses segments dans d'autres systèmes informatiques, souvent par e-mail.
- **Autres** : Virus/programmes malveillants n'entrant dans aucune des catégories de types de virus/programmes malveillants.

Spywares et graywares

Les ordinateurs clients courent des risques à cause de menaces potentielles autres que les virus/programmes malveillants. Les spywares/graywares sont des applications ou fichiers non classés en tant que virus ou chevaux de Troie, mais qui peuvent toutefois avoir un effet négatif sur les performances des ordinateurs de votre réseau. Ils font courir un risque significatif à votre entreprise sur le plan de la sécurité et de la confidentialité et peuvent avoir des conséquences judiciaires. Les spywares/graywares réalisent souvent des actions variées non souhaitées et menaçantes qui irritent les utilisateurs avec des fenêtres pop-up, enregistrent les séquences de frappe des touches du clavier et exposent les failles de l'ordinateur à des attaques.

Si vous découvrez une application ou un fichier que OfficeScan ne peut pas détecter comme étant un grayware, mais que vous jugez qu'il en est un, envoyez-le à Trend Micro à l'adresse suivante :

http://subwiz.trendmicro.com/SubWiz

Types de spywares/graywares

- **Programme espion** : rassemble des données telles que des noms d'utilisateur de comptes et des mots de passe pour les transmettre à des tiers.
- **Programmes publicitaires** : affiche des publicités et rassemble des données telles que les préférences de navigation de l'utilisateur afin de cibler les publicités destinées à cet utilisateur via un navigateur Web.
- **Numéroteur** : modifie les paramètres Internet de l'ordinateur et oblige un ordinateur à composer des numéros de téléphone préconfigurés à l'aide d'un modem. Ce sont souvent des numéros de services téléphoniques facturés à l'utilisation (pay-per-call) ou internationaux qui peuvent entraîner une dépense significative pour votre entreprise.
- **Canular** : entraîne un comportement anormal de l'ordinateur, comme la fermeture et l'ouverture du tiroir de CD-ROM et l'affichage de nombreuses boîtes de message.
- **Outil de piratage** : aide les pirates informatiques à s'infiltrer sur les ordinateurs.
- **Outil d'accès à distance** : aide les pirates informatiques à accéder à distance à plusieurs ordinateurs et à les contrôler.
- **Application de piratage des mots de passe** : aide les pirates informatiques à déchiffrer des noms d'utilisateurs et des mots de passe.
- **Autres** : Autres types de programmes potentiellement malveillants.

Comment les spywares/graywares s'infiltrent-t-ils sur le réseau

Les spywares/graywares s'introduisent généralement dans un réseau d'entreprise lorsque les utilisateurs téléchargent des programmes légitimes dont le module d'installation contient des applications de graywares. La plupart des programmes proposent un contrat de licence utilisateur final (CLUF) que l'utilisateur est tenu d'accepter avant de lancer la procédure de téléchargement. Ce contrat de licence inclut des informations relatives à l'application et à sa fonction de collecte de données personnelles ; toutefois,

les utilisateurs négligent souvent ces informations ou ne comprennent pas la terminologie juridique.

Risques et menaces potentiels

La présence de spywares et d'autres types de graywares sur le réseau est susceptible de donner lieu à ce qui suit :

- **Réduction des performances de l'ordinateur** : Afin d'exécuter leurs tâches, les applications de spywares/graywares requièrent souvent une grande partie des ressources du processeur et de la mémoire du système.
- **Davantage de blocages liés au navigateur Web** : Certains types de graywares, tels que les adwares, affichent souvent des informations dans un cadre ou dans la fenêtre du navigateur. Selon le mode d'interaction du code de ces applications avec les processus système, les graywares peuvent parfois provoquer une panne ou un blocage des navigateurs ; un redémarrage du système s'impose parfois.
- **Diminution de l'efficacité de l'utilisateur** : Le fait de devoir fermer fréquemment les fenêtres publicitaires contextuelles et de devoir gérer les effets négatifs des canulars détourne les utilisateurs inutilement de leurs tâches principales.
- **Dégradation de la bande passante du réseau** : Souvent les applications spyware/grayware transmettent régulièrement les données collectées à d'autres applications en cours d'exécution sur le réseau ou à l'extérieur de celui-ci.
- **Perte d'informations personnelles et de l'entreprise** : Les données que les applications de spywares/graywares rassemblent ne sont pas toutes aussi inoffensives qu'une liste de sites Web consultés par les utilisateurs. Le spyware/grayware est également susceptible de recueillir des informations d'identification, comme celles utilisées pour accéder aux comptes bancaires en ligne et aux réseaux d'entreprise.
- **Risque accru de responsabilité civile** : En cas de piratage des ressources informatiques du réseau, les pirates peuvent utiliser vos ordinateurs clients pour lancer des attaques ou installer des programmes de spywares/graywares sur des ordinateurs situés en dehors du réseau. L'utilisation des ressources du réseau pour des activités de ce genre peut rendre l'entreprise responsable juridiquement des dommages occasionnés aux autres parties.

Protection contre les spywares/graywares et autres menaces

Vous pouvez prendre de nombreuses mesures pour éviter l'installation de spywares/graywares sur votre ordinateur. Trend Micro propose d'effectuer les opérations suivantes :

- Configurez tous les types de scans (scan manuel, scan en temps réel, scan programmé et scan immédiat) pour rechercher des fichiers et applications de spywares/graywares et les supprimer. Voir la *Types de scan à la page 6-14* pour plus d'informations.
- Formez les utilisateurs de postes clients à effectuer les opérations suivantes :
  - Lire le contrat de licence utilisateur final (CLUF) et la documentation fournie avec les applications téléchargées et installées sur les ordinateurs.
  - Cliquez sur **Non** dans chaque boîte de dialogue demandant l'autorisation de télécharger et d'installer des logiciels à moins que les utilisateurs clients ne soient certains que l'auteur du logiciel et le site Web utilisés sont dignes de confiance.
  - Ignorer tout e-mail commercial non sollicité (spam), particulièrement si le spam demande aux utilisateurs de cliquer sur un bouton ou un lien hypertexte.
- Configurez les paramètres du navigateur web afin d'assurer un niveau de sécurité strict. Trend Micro recommande de configurer les navigateurs Web pour qu'ils demandent confirmation aux utilisateurs avant d'installer des contrôles ActiveX.
- Si vous utilisez Microsoft Outlook, configurez les paramètres de sécurité de façon à ce qu'Outlook ne télécharge pas automatiquement des éléments HTML, tels que les images envoyées dans les messages de spam.
- N'autorisez pas l'utilisation de services de partage de fichiers Peer-to-Peer. Les applications de spywares ou autres graywares peuvent se cacher derrière d'autres types de fichiers que les utilisateurs peuvent souhaiter télécharger tels que les fichiers musicaux MP3.
- Examinez régulièrement les logiciels installés sur vos ordinateurs agents et recherchez les applications pouvant être des spywares ou autres graywares.

- Maintenez à jour votre système d'exploitation Windows avec les patchs les plus récents de Microsoft. Consultez le site Web de Microsoft pour plus d'informations.

Méthodes de scan

Les clients OfficeScan peuvent utiliser l'une des deux méthodes de scan pour rechercher les risques de sécurité. Les méthodes de scan sont le Smart Scan et le scan traditionnel.

- **Smart Scan**

  Dans ce document, les clients utilisant le Smart Scan sont appelés les **clients Smart Scan**. Les clients Smart Scan bénéficient de scans locaux et de requêtes en ligne fournis par les services de File Reputation.

- **Scan traditionnel**

  Les clients n'utilisant pas le Smart Scan sont appelés les **clients de scan traditionnel**. Un client scan conventionnel stocke tous les composants OfficeScan sur l'ordinateur client et scanne tous les fichiers localement.

Méthode de scan par défaut

Dans cette version d'OfficeScan, Smart Scan est la méthode de scan par défaut pour les nouvelles installations. En d'autres termes, si vous effectuez une nouvelle installation du serveur OfficeScan sans avoir changé la méthode de scan dans la console Web, tous les clients gérés par le serveur utiliseront Smart Scan.

Si vous mettez à niveau le serveur OfficeScan à partir d'une version antérieure et que la mise à niveau automatique des clients est activée, tous les clients gérés par le serveur utiliseront toujours la méthode de scan configurée avant la mise à niveau. Par exemple, une mise à niveau depuis OfficeScan 8.x, qui n'accepte que le scan traditionnel, signifie que tous les clients continueront d'utiliser le scan traditionnel après la mise à niveau. Si vous effectuez une mise à niveau depuis OfficeScan 10, qui prend en charge le Smart Scan et le scan traditionnel, tous les clients ayant effectué la mise à niveau et utilisant le Smart Scan continueront de l'utiliser, et tous ceux utilisant le scan traditionnel continueront d'utiliser ce dernier.

Comparaison des méthodes de scan

Le tableau suivant compare les deux méthodes de scan :

TABLEAU 6-1. Comparaison entre le scan traditionnel et Smart Scan

BASE DE COMPARAISON	SCAN TRADITIONNEL	SMART SCAN
Disponibilité	Disponible dans cette version d'OfficeScan et toutes les précédentes	Disponible à partir d'OfficeScan 10
Comportement de scan	Le client scan conventionnel effectue le scan sur l'ordinateur local.	• Le client Smart Scan effectue le scan sur l'ordinateur local. • S'il ne parvient pas à déterminer le risque auquel le fichier est exposé durant le scan, il vérifie le risque en envoyant une requête de scan à une source Smart Protection. • Le client met en mémoire cache le résultat de la requête de scan pour améliorer les performances du scan.
Composants utilisés et mis à jour	Tous les composants disponibles sur la source de mise à jour, hormis Smart Scan Agent Pattern	Tous les composants disponibles sur la source de mise à jour, hormis le fichier de signatures de virus et le celui de surveillance active des spywares
Source de mise à jour habituelle	Serveur OfficeScan	Serveur OfficeScan

Changement de la méthode de scan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.

2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Méthodes de scan**.
4. Sélectionnez **Scan traditionnel** ou **Smart Scan**.
5. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Passage de Smart Scan au scan traditionnel

Lorsque vous faites passer des clients au scan traditionnel, tenez compte de ce qui suit :

1. **Nombre de clients devant basculer**

   Le basculement simultané d'un nombre de clients relativement réduit permet d'utiliser efficacement les ressources le serveur OfficeScan et les ressources Smart Protection Server. Ces serveurs peuvent effectuer d'autres tâches critiques lorsque les clients changent de méthode de scan.

2. **Synchronisation**

   Lorsqu'ils repassent au scan traditionnel, les clients téléchargeront probablement la version complète du fichier de signatures de virus et des signatures de surveillance active de spywares à partir du serveur OfficeScan. Ces fichiers de signatures ne sont utilisés que par les clients de scan traditionnel.

   Prévoyez d'effectuer le basculement pendant les heures creuses pour vous assurer que le processus de téléchargement se termine rapidement. Prévoyez également

d'effectuer le basculement lorsqu'aucune mise à jour de client n'est programmée à partir du serveur. De plus, désactivez temporairement l'option «Mettre à jour» sur les clients et réactivez-la lorsque les clients ont basculé vers Smart Scan.

3. **Paramètres de l'arborescence des clients**

   La méthode de scan est un paramètre détaillé qui peut être défini au niveau de la racine, du domaine ou d'un client individuel. Lorsque vous passez au scan traditionnel, vous pouvez :

   - Créer un nouveau domaine de l'arborescence des clients et définir le scan traditionnel comme sa méthode de scan. Tout client que vous déplacez vers ce domaine utilisera le scan traditionnel. Lorsque vous déplacez le client, activez le paramètre **Appliquer les paramètres du nouveau domaine aux clients sélectionnés**.
   - Sélectionnez un domaine et configurez-le pour utiliser le scan traditionnel. Les clients Smart Scan appartenant au domaine passeront au scan traditionnel.
   - Sélectionnez un ou plusieurs clients Smart Scan d'un domaine et faites-les passer au scan traditionnel.

Remarque

Tout changement de méthode de scan du domaine remplace la méthode que vous avez configurée pour des clients individuels.

Passage du scan traditionnel à Smart Scan

Si vous faites basculer les clients du scan traditionnel vers le Smart Scan, assurez-vous d'avoir configuré les Services Smart Protection. Pour obtenir des informations détaillées, voir *Configuration des services Smart Protection à la page 3-13*.

Le tableau suivant donne d'autres éléments à prendre en compte lorsque vous basculez vers le Smart Scan :

TABLEAU 6-2. Éléments à prendre en compte lorsque vous basculez vers Smart Scan

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Fonctionnalités et fonctions non disponibles	Les clients Smart Scan ne peuvent pas signaler les informations relatives à Smart Scan Pattern et Smart Scan Agent Pattern au serveur Policy Server.
Licence du produit	Pour utiliser Smart Scan, assurez-vous que vous avez activé les licences des services suivants et que ces licences n'ont pas expiré : • Antivirus • Réputation de sites Web et anti-spyware
Serveur OfficeScan	Vérifiez que les clients peuvent se connecter au serveur OfficeScan. Seuls les clients en ligne seront invités à passer à Smart Scan. Les clients hors ligne sont notifiés lorsqu'ils sont en ligne. Les clients itinérants sont notifiés lorsqu'ils sont en ligne ou, si le client a le privilège de mise à jour programmée, lorsqu'une mise à jour programmée s'exécute. Vérifiez également que le serveur OfficeScan possède les tout derniers composants car les clients Smart Scan doivent télécharger le Smart Scan Agent Pattern à partir du serveur. Pour mettre à jour les composants, reportez-vous à *Mises à jour du serveur OfficeScan à la page 5-15*.
Nombre de clients devant basculer	Le basculement simultané d'un nombre de clients relativement réduit permet d'utiliser efficacement les ressources du serveur OfficeScan. Le serveur OfficeScan peut effectuer d'autres tâches critiques lorsque les clients changent de méthode de scan.

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Synchronisation	Lorsqu'ils passent à Smart Scan pour la première fois, les clients doivent télécharger la version complète du fichier Smart Scan Agent Pattern à partir du serveur OfficeScan. Le fichier Smart Scan Pattern n'est utilisé que par les clients Smart Scan. Prévoyez d'effectuer le basculement pendant les heures creuses pour vous assurer que le processus de téléchargement se termine rapidement. Prévoyez également d'effectuer le basculement lorsqu'aucune mise à jour de client n'est programmée à partir du serveur. De plus, désactivez temporairement l'option «Mettre à jour» sur les clients et réactivez-la lorsque les clients ont basculé vers Smart Scan.
Paramètres de l'arborescence des clients	La méthode de scan est un paramètre détaillé qui peut être défini au niveau de la racine, du domaine ou d'un client individuel. Lorsque vous passez à Smart Scan, vous pouvez: • Créer un nouveau domaine de l'arborescence client et définir Smart Scan comme sa méthode de scan. Tout client que vous déplacez vers ce domaine utilisera Smart Scan. Lorsque vous déplacez le client, activez le paramètre **Appliquer les paramètres du nouveau domaine aux clients sélectionnés**. • Sélectionnez un domaine et configurez-le pour utiliser Smart Scan. Les clients de scan traditionnel appartenant au domaine passeront à Smart Scan. • Sélectionnez un ou plusieurs clients de scan traditionnel dans un domaine et faites-les passer à Smart Scan. **Remarque** Tout changement de méthode de scan du domaine remplace la méthode que vous avez configurée pour des clients individuels.

Éléments à prendre en compte	Détails
Prise en charge d'IPv6	Les clients Smart Scan envoient des requêtes de scan aux sources Smart Protection. Un client Smart Scan IPv6 pur ne peut envoyer directement de requêtes à des sources IPv4 pures telles que : • Smart Protection Server 2.0 (intégré ou autonome) **Remarque** IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5. • Trend Micro Smart Protection Network De même, un client Smart Scan IPv4 pur ne peut envoyer de requêtes à des serveurs Smart Protection IPv6 purs. Un serveur proxy double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients Smart Scan de se connecter aux sources.

Types de scan

OfficeScan propose les types de scan suivants afin de protéger les ordinateurs clients OfficeScan contre les risques de sécurité :

Tableau 6-3. Types de scan

Type de scan	Description
Scan en temps réel	Scanne automatiquement un fichier sur l'ordinateur dès sa réception, son ouverture, son téléchargement, sa copie ou sa modification Voir *Scan en temps réel à la page 6-15* pour obtenir des informations détaillées.

TYPE DE SCAN	DESCRIPTION
Scan manuel	désigne un scan initié par l'utilisateur qui analyse un fichier ou un ensemble de fichiers à la demande de ce dernier. Voir *Scan manuel à la page 6-18* pour obtenir des informations détaillées.
Scan programmé	Désigne un scan automatique des fichiers de l'ordinateur selon le programme configuré par l'administrateur ou par l'utilisateur Voir *Scan programmé à la page 6-20* pour obtenir des informations détaillées.
Scan immédiat	Désigne un scan lancé par l'administrateur qui scanne les fichiers sur un ou plusieurs ordinateurs cibles Voir *Scan immédiat à la page 6-23* pour obtenir des informations détaillées.

Scan en temps réel

Le scan en temps réel s'effectue en continu. Lors de la réception, de l'ouverture, du téléchargement, de la copie ou de la modification d'un fichier, le scan en temps réel recherche les risques pour la sécurité. Si OfficeScan ne détecte aucun risque de sécurité, le fichier demeure à sa place et les utilisateurs peuvent y accéder. Si un risque de sécurité ou un programme malveillant probable est détecté, OfficeScan affiche un message de notification avec le nom du fichier infecté et le risque spécifique lié à la sécurité.

Remarque

Pour modifier le message de notification, ouvrez la console Web et accédez à **Notifications** > **Notifications aux utilisateurs clients**.

Configurez et appliquez les paramètres du scan en temps réel à un ou plusieurs clients et domaines, ou à tous les clients que le serveur gère.

Configuration des paramètres de scan en temps réel

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan en temps réel**.
4. Dans l'onglet **Cible**, sélectionnez les options suivantes :
   - Activer le scan antivirus/programme malveillant
   - Activer le scan antispyware/grayware

   Remarque

   Si vous désactivez le scan antivirus/programmes malveillants, le scan anti-spywares/graywares se désactive également. Au cours d'une épidémie virale, le scan en temps réel ne peut pas être désactivé (ou sera activé automatiquement s'il était désactivé au départ) pour empêcher les virus de modifier ou de supprimer les fichiers et les dossiers sur les ordinateurs clients.
5. Configurez les critères suivants pour le scan :
   - *Action des utilisateurs sur les fichiers à la page 6-27*
   - *Fichiers à scanner à la page 6-27*
   - *Paramètres de scan à la page 6-28*
   - *Exclusions de scan à la page 6-31*
6. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 6-4. Actions du scan en temps réel

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 6-38* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 6-39* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 6-40* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 6-36*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 6-40* • *Sauvegardez les fichiers avant nettoyage à la page 6-42* • *Damage Cleanup Services à la page 6-42* • *Afficher un message de notification lorsqu'un virus/ programme malveillant est détecté à la page 6-44* • *Afficher un message de notification lorsqu'un virus/ programme malveillant potentiel est détecté à la page 6-44*
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 6-48* Action de spywares/graywares supplémentaires : • *Afficher un message de notification lorsqu'un spyware/grayware est détecté à la page 6-49*

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Scan manuel

Le scan manuel est un scan à la demande qui démarre immédiatement après avoir été lancé dans la console client OfficeScan par l'utilisateur. La durée du scan dépend du nombre de fichiers spécifiés pour le scan et des ressources matérielles de l'ordinateur client OfficeScan.

Configurez et appliquez les paramètres de scan manuel à un ou plusieurs clients et domaines, ou à tous les clients que le serveur gère.

Configuration d'un scan manuel

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan manuel**.
4. Dans l'onglet **Cible**, configurez ce qui suit :
   - *Fichiers à scanner à la page 6-27*
   - *Paramètres de scan à la page 6-28*

- *Utilisation de l'UC à la page 6-30*
- *Exclusions de scan à la page 6-31*

5. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 6-5. Actions du scan manuel

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 6-38* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 6-39* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 6-40* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 6-36*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 6-40* • *Sauvegardez les fichiers avant nettoyage à la page 6-42* • *Damage Cleanup Services à la page 6-42*
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 6-48*

6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les

domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Scan programmé

Un scan programmé démarre automatiquement aux date et heure programmées. Utilisez le scan programmé pour automatiser les scans de routine sur le client et améliorer l'efficacité de votre gestion de scan.

Configurez et appliquez les paramètres de scan programmé à un ou plusieurs clients et domaines, ou à tous les clients que le serveur gère.

Configuration d'un scan programmé

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan programmé**.
4. Dans l'onglet **Cible**, sélectionnez les options suivantes :
   - **Activer le scan antivirus/programme malveillant**
   - **Activer le scan antispyware/grayware**

Remarque

Si vous désactivez le scan antivirus/programmes malveillants, le scan anti-spywares/graywares se désactive également.

5. Configurez les critères suivants pour le scan :
   - *Programmation à la page 6-30*
   - *Fichiers à scanner à la page 6-27*
   - *Paramètres de scan à la page 6-28*
   - *Utilisation de l'UC à la page 6-30*
   - *Exclusions de scan à la page 6-31*
6. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 6-6. Actions de scan programmé

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 6-38* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 6-39* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 6-40* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 6-36*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 6-40* • *Sauvegardez les fichiers avant nettoyage à la page 6-42* • *Damage Cleanup Services à la page 6-42* • *Afficher un message de notification lorsqu'un virus/ programme malveillant est détecté à la page 6-44* • *Afficher un message de notification lorsqu'un virus/ programme malveillant potentiel est détecté à la page 6-44*
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 6-48* Action de spywares/graywares supplémentaires : • *Afficher un message de notification lorsqu'un spyware/grayware est détecté à la page 6-49*

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Scan immédiat

Le scan immédiat est lancé à distance par un administrateur OfficeScan via la console Web et peut concerner un ou plusieurs ordinateurs clients.

Configurez et appliquez les paramètres du scan immédiat à un ou plusieurs clients et domaines, ou à tous les clients que le serveur gère.

Configuration des paramètres de scan immédiat

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan immédiat**.
4. Dans l'onglet **Cible**, sélectionnez les options suivantes :
   - **Activer le scan antivirus/programme malveillant**
   - **Activer le scan antispyware/grayware**

Remarque

Si vous désactivez le scan antivirus/programmes malveillants, le scan anti-spywares/graywares se désactive également.

5. Configurez les critères suivants pour le scan :

   - *Fichiers à scanner à la page 6-27*
   - *Paramètres de scan à la page 6-28*
   - *Utilisation de l'UC à la page 6-30*
   - *Exclusions de scan à la page 6-31*

6. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 6-7. Actions de scan immédiat

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 6-38* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 6-39* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 6-40* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 6-36*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 6-40* • *Sauvegardez les fichiers avant nettoyage à la page 6-42* • *Damage Cleanup Services à la page 6-42*

ACTION	RÉFÉRENCE
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 6-48*

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Exécution du scan immédiat

Lancez un Scan immédiat sur les ordinateurs susceptibles d'être infectés.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Tâches** > **Scan immédiat**.
4. Pour modifier les paramètres de **scan immédiat** préconfigurés avant le lancement du scan, cliquez sur **Paramètres**.

   L'écran **Paramètres de scan immédiat** apparaît. Voir *Scan immédiat à la page 6-23* pour obtenir des informations détaillées.
5. Dans l'arborescence client, sélectionnez les clients devant exécuter un scan et cliquez sur **Lancer un scan immédiat**.

Remarque

Si vous ne sélectionnez aucun client, OfficeScan envoie automatiquement une notification à tous les clients de l'arborescence client.

Le serveur envoie une notification aux clients.

6. Vérifiez l'état de notification et assurez-vous que tous les clients ont reçu une notification.

7. Cliquez sur **Sélectionner les ordinateurs non informés**, puis sur **Lancez le scan immédiat** pour envoyer immédiatement une nouvelle notification aux clients non informés.

   Exemple : Nombre total de clients : 50

TABLEAU 6-8. Scénarios concernant les clients non informés

SÉLECTION DANS L'ARBORESCENCE CLIENT	CLIENTS INFORMÉS (APRÈS SÉLECTION DE L'OPTION «LANCER UN SCAN IMMÉDIAT»)	CLIENTS NON INFORMÉS
Aucun (la totalité des 50 clients est sélectionnée automatiquement)	35 clients sur 50	15 clients
Sélection manuelle (45 clients sur 50 sélectionnés)	40 clients sur 45	5 clients + 5 autres clients non inclus dans la sélection manuelle

8. Cliquez sur **Arrêter la notification** pour qu'OfficeScan arrête d'envoyer des notifications aux clients recevant actuellement des notifications. Les clients déjà informés et dont le processus de scan est en cours ignorent cette commande.

9. Pour les clients dont le processus de scan a commencé, cliquez sur **Arrêter le scan immédiat** pour leur envoyer une notification leur demandant d'arrêter le scan.

Paramètres communs à tous les types de scan

Pour chaque type de scan, configurez trois ensembles de paramètres : Critères de scan, exclusions de scan et actions de scan. Déployez ces paramètres sur un ou plusieurs clients et domaines, ou sur tous les clients que le serveur gère.

Critères de scan

Spécifiez les fichiers qu'un type de scan donné doit scanner en utilisant des attributs de fichier tels que le type de fichier et l'extension. Spécifiez également les conditions qui déclencheront le scan. Par exemple, configurez le scan en temps réel pour scanner chaque fichier après son téléchargement sur l'ordinateur.

Action des utilisateurs sur les fichiers

Choisissez les actions sur les fichiers qui déclenchent le scan en temps réel. Sélectionnez l'une des options suivantes :

- **Scanner les fichiers en cours de création/modification** : scanne les nouveaux fichiers parvenant dans l'ordinateur (par exemple, après leur téléchargement) ou les fichiers en cours de modification
- **Scanner les fichiers en cours de récupération** : scanne les fichiers lorsqu'ils sont ouverts
- **Scanner les fichiers en cours de création/modification et de récupération**

Par exemple, si la troisième option est sélectionnée, un nouveau fichier téléchargé sur l'ordinateur est scanné et reste à son emplacement actuel si aucun risque de sécurité n'est détecté. Le même fichier est scanné lorsqu'un utilisateur l'ouvre et, s'il a modifié ce fichier, avant l'enregistrement des modifications.

Fichiers à scanner

Sélectionnez l'une des options suivantes :

- **Tous les fichiers scannables** : Scanner tous les fichiers
- **Types de fichiers scannés par IntelliScan** : scanne uniquement les fichiers connus pour contenir potentiellement du code malveillant, y compris ceux

dissimulés sous une extension inoffensive. Voir *IntelliScan à la page C-6* pour obtenir des informations détaillées.

- **Fichiers avec certaines extensions** : scanne uniquement les fichiers dont les extensions figurent dans la liste des extensions de fichier. Ajoutez de nouvelles extensions ou supprimez des extensions existantes.

Paramètres de scan

Sélectionnez une ou plusieurs des options suivantes :

- **Scanner la disquette pendant l'arrêt du système** : scanne les disquettes à la recherche de virus d'amorce avant l'arrêt de l'ordinateur. Ceci évite que des virus ou des programmes malveillants ne s'exécutent lorsqu'un utilisateur redémarre l'ordinateur à partir de la disquette.
- **Scanner les dossiers cachés** : permet à OfficeScan de détecter, puis de scanner les dossiers masqués sur l'ordinateur au cours d'un scan manuel
- **Scanner les lecteurs de réseau** : scanne les lecteurs ou les dossiers du réseau mappés sur l'ordinateur client OfficeScan au cours du scan manuel ou du scan en temps réel.
- **Scanner le secteur d'amorçage du périphérique de stockage amovible après sa connexion** : scanne automatiquement uniquement le secteur d'amorçage d'un périphérique de stockage USB à chaque fois que l'utilisateur le connecte (scan en temps réel).
- **Scanner tous les fichiers des périphériques de stockage amovibles lors de leur connexion** : scanne automatiquement l'ensemble des fichiers d'un périphérique de stockage USB à chaque fois que l'utilisateur le connecte (scan en temps réel).
- **Scanner les fichiers compressés**: permet à OfficeScan de scanner un nombre maximum spécifié de couches de compression et de ne pas scanner les couches supplémentaires. OfficeScan nettoie aussi ou supprime les fichiers infectés dans les fichiers compressés. Par exemple, si le maximum que vous avez choisi est de deux couches et qu'un fichier à scanner comprend six couches, OfficeScan analyse deux couches sans analyser les quatre suivantes. Si un fichier compressé contient des risques de sécurité, OfficeScan le nettoie ou le supprime.

Remarque

OfficeScan traite les fichiers Microsoft Office 2007 au format Office Open XML comme étant des fichiers compressés. Office Open XML, format de fichier des applications Office 2007, utilise les technologies de compression ZIP. Si vous voulez que les fichiers créés à l'aide de ces applications soient scannés pour détecter les virus/programmes malveillants, vous devez activer le scan des fichiers compressés.

- **Scanner les objets OLE** : lorsqu'un fichier contient plusieurs couches Object Linking and Embedding (OLE), OfficeScan scanne le nombre de couches que vous spécifiez et ignore les autres.

  Tous les clients OfficeScan gérés par le serveur vérifient ce paramètre lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat. Chaque couche fait l'objet d'un scan antivirus/programme malveillant et antispyware/grayware.

  Par exemple :

  Le nombre de couches que vous spécifiez est de 2. Un fichier intègre un document Microsoft Word (première couche), qui comporte une feuille de calcul Microsoft Excel (deuxième couche), qui contient un fichier `.exe` (troisième couche). OfficeScan effectuera le scan du document Word ainsi que de la feuille de calcul Excel et ignorera le fichier `.exe`.

  - **Détecter le code d'exploitation dans les fichiers OLE**: La détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office.

    Remarque

    Le nombre spécifié de couches s'applique à la fois aux options **Scanner les objets OLE** et **Détecter le code d'exploitation**.

- **Activer IntelliTrap** : détecte et supprime les virus/programmes malveillants des fichiers exécutables compressés. Cette option est uniquement disponible pour le scan en temps réel. Voir *IntelliTrap à la page C-7* pour obtenir des informations détaillées.

- **Scanner la zone d'amorçage** : recherche les virus/programmes malveillants dans le secteur d'amorçage du disque dur de l'ordinateur client lors du scan manuel, du scan programmé et du scan immédiat.

Utilisation de l'UC

OfficeScan peut s'interrompre entre le scan d'un fichier et le scan du suivant. Ce paramètre est utilisé lors du scan manuel, du scan programmé et du scan immédiat.

Sélectionnez l'une des options suivantes :

- **Élevé** : aucune interruption entre les scans
- **Moyen** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50 % et pas d'interruption si elle est de 50 % ou moins
- **Faible** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 20% et pas d'interruption si elle est de 20% ou moins

Si vous choisissez Moyen ou Faible, lorsque le scan démarre et si la consommation de l'UC respecte le seuil (50% ou 20%), OfficeScan ne s'interrompt pas entre les scans, ce qui se traduit par des temps de scan plus rapides. OfficeScan utilise plus de ressources d'UC au cours du processus mais du fait que la consommation de l'UC est optimale, les performances de l'ordinateur ne sont pas affectées de façon significative. Lorsque la consommation de l'UC commence à dépasser le seuil, OfficeScan s'interrompt pour réduire l'utilisation de l'UC, et reprend lorsque la consommation revient sous le seuil indiqué.

Si vous choisissez Élevé, OfficeScan ne vérifie pas la consommation réelle de l'UC et scanne les fichiers sans interruption.

Programmation

Configurez la fréquence (quotidienne, hebdomadaire ou mensuelle) et l'heure à laquelle le scan programmé démarre.

Pour les scans programmés mensuellement, vous pouvez choisir un jour particulier d'un mois ou un jour de la semaine ainsi que l'ordre de son occurrence.

- **Un jour particulier d'un mois** : Sélectionnez un jour entre le 1er et le 31. Si vous avez sélectionnez le 29, le 30 ou le 31 et si un mois ne comporte pas ce jour, OfficeScan exécute le scan programmé le dernier jour du mois. Par conséquent :

- Si vous avez sélectionné 29, le scan programmé s'exécute le 28 février (sauf en cas d'année bissextile) et le 29e jour de tous les autres mois.
- Si vous avez sélectionné 30, le scan programmé s'exécute le 28 ou le 29 février et le 30ème jour de tous les autres mois.
- Si vous avez sélectionné 31, le scan programmé s'exécute le 28 ou le 29 février, le 30 avril, le 30 juin, le 30 septembre, le 30 novembre et le 31ème jour de tous les autres mois.

- **Un jour de la semaine et l'ordre de son occurrence** : Un jour de la semaine se produit quatre ou cinq fois par mois. Par exemple, il y a généralement quatre lundis chaque mois. Indiquez un jour de la semaine et l'ordre dans lequel il se produit au cours d'un mois. Par exemple, choisissez d'exécuter le scan programmé le second lundi de chaque mois. Si vous choisissez la cinquième occurrence d'un jour de la semaine, et si ce jour n'existe pas au cours d'un mois donné, le scan s'exécute à la quatrième occurrence.

Exclusions de scan

Configurez des exclusions de scan afin d'améliorer les performances du scan et d'ignorer les fichiers provoquant de fausses alertes. Lorsqu'un type de scan particulier s'exécute, OfficeScan examine la liste d'exclusion de scan pour déterminer les fichiers de l'ordinateur qui seront exclus de la recherche de virus/programmes malveillants et de spywares/graywares.

Lorsque vous activez des exclusions de scan, OfficeScan ne scanne pas un fichier dans les conditions suivantes :

- Le fichier se trouve dans un répertoire donné (ou dans l'un de ses sous-répertoires).
- Le nom du fichier correspond à l'un de ceux de la liste d'exclusion.
- L'extension du fichier correspond à l'une de celles de la liste d'exclusion.

Exceptions avec caractères génériques

Les listes d'exclusion de scan pour les fichiers et les répertoires prennent en charge l'utilisation des caractères génériques. Utilisez « ? » pour remplacer un caractère et « * » pour en remplacer plusieurs.

Utilisez les caractères génériques avec précaution. L'utilisation d'un caractère erroné peut exclure des fichiers ou des répertoires incorrects. Par exemple, `C:\*` exclut l'intégralité du lecteur `C:\`.

TABLEAU 6-9. Exclusions de scan avec des caractères génériques

VALEUR	EXCLUS	NON EXCLUS

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	`c:\doc.txt`	`c:\directory\file\doc.txt` `c:\directories\files\document.txt`
`[]`	Non pris en charge	Non pris en charge
`*.*`	Non pris en charge	Non pris en charge

Liste d'exclusion de scan (répertoires)

OfficeScan ne scanne pas l'ensemble des fichiers contenus dans un répertoire spécifique de l'ordinateur. Vous pouvez spécifier au maximum 250 répertoires.

Remarque

Une fois qu'un répertoire donné est exclu des actions de scans, OfficeScan exclut également automatiquement l'ensemble des sous-répertoires de ce répertoire.

Vous pouvez également choisir l'option **Exclure les répertoires dans lesquels sont installés des produits Trend Micro**. Si vous sélectionnez cette option, OfficeScan exclut automatiquement du scan les répertoires des produits Trend Micro suivants :

- <*Dossier d'installation du serveur*>
- ScanMail™ for Microsoft Exchange (toutes les versions sauf la version 7). Si vous utilisez la version 7, ajoutez les dossiers suivants à la liste des exclusions :
  - `\Smex\Temp`
  - `\Smex\Storage`
  - `\Smex\ShareResPool`
- ScanMail eManager™ 3.11, 5.1, 5.11 et 5.12
- ScanMail for Lotus Notes™ eManager NT
- InterScan™ Messaging Security Suite
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan VirusWall 3.53
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x

Si vous disposez d'un produit Trend Micro NON répertorié dans la liste, ajoutez manuellement les répertoires de ce produit à la liste d'exclusion de scan.

Configurez également OfficeScan pour exclure les répertoires Microsoft Exchange 2000/2003 en accédant à la section **Paramètres de scan** de **Ordinateurs en réseau** > **Gestion des clients**. Si vous utilisez Microsoft Exchange 2007 ou une version plus récente, ajoutez manuellement le répertoire à la liste d'exclusion de scan. Reportez-vous au site suivant pour obtenir des informations détaillées sur les exclusions de scan :

http://technet.microsoft.com/en-us/library/bb332342.aspx

Lorsque vous configurez la liste de fichiers, choisissez l'une des options suivantes :

- **Conservation de la liste d'exclusion de l'ordinateur client** : Il s'agit de la sélection par défaut. Si vous effectuez des modifications dans la liste d'exclusion et que cette option est activée, vous ne pourrez pas sauvegarder les modifications. Cette option empêche d'écraser involontairement une liste d'exclusion existante d'un client. Si vous voulez déployer les modifications effectuées, sélectionnez l'une des autres options.
- **Remplacement de la liste d'exclusion de l'ordinateur client**: Cette option supprime toute la liste d'exclusion et la remplace par la liste que vous venez de configurer. Si vous choisissez cette option, OfficeScan affiche une alerte. Pour poursuivre, vous devez cliquer sur **Ok** dans la fenêtre du message.
- **Ajout du chemin d'accès à la liste d'exclusion de l'ordinateur client**: Cette option ajoute les éléments dans la liste que vous venez de configurer à la liste d'exclusion existante du client. Si un élément existe déjà dans la liste d'exclusion du client, le client ignore l'élément.
- **Suppression du chemin d'accès de la liste d'exclusion de l'ordinateur client**: Le client supprime un élément de sa liste d'exclusion s'il correspond à un élément de la liste que vous venez de configurer.

Liste d'exclusion de scan (fichiers)

OfficeScan ne scanne pas un fichier si son nom correspond à l'un de ceux de la liste d'exclusion. Si vous souhaitez exclure un fichier qui se trouve à un emplacement spécifique de l'ordinateur, indiquez son chemin d'accès, par exemple `C:\Temp\sample.jpg`.

Vous pouvez spécifier au maximum 250 fichiers.

Lorsque vous configurez la liste de fichiers, choisissez l'une des options suivantes :

- **Conservation de la liste d'exclusion de l'ordinateur client** : il s'agit de la sélection par défaut. Si vous effectuez des modifications dans la liste d'exclusion et que cette option est activée, vous ne pourrez pas sauvegarder les modifications. Cette option empêche d'écraser involontairement une liste d'exclusion existante

d'un client. Si vous voulez déployer les modifications effectuées, sélectionnez l'une des autres options.

- **Remplacement de la liste d'exclusion de l'ordinateur client** : cette option supprime toute la liste d'exclusion et la remplace par la liste que vous venez de configurer. Si vous choisissez cette option, OfficeScan affiche une alerte. Pour poursuivre, vous devez cliquer sur **Ok** dans la fenêtre du message.
- **Ajout du chemin d'accès à la liste d'exclusion de l'ordinateur client** : cette option ajoute les éléments dans la liste que vous venez de configurer à la liste d'exclusion existante du client. Si un élément existe déjà dans la liste d'exclusion du client, le client ignore l'élément.
- **Suppression du chemin d'accès de la liste d'exclusion de l'ordinateur client** : le client supprime un élément de sa liste d'exclusion s'il correspond à un élément de la liste que vous venez de configurer.

Liste d'exclusion de scan (extensions de fichier)

OfficeScan ne scanne pas un fichier si son extension correspond à l'une de celles de la liste d'exclusion. Vous pouvez spécifier au maximum 250 extensions de fichier. Le point (.) n'est pas nécessaire devant l'extension.

Pour le scan en temps réel, utilisez un astérisque (*) comme caractère générique lorsque vous spécifiez des extensions. Par exemple, si vous ne souhaitez pas scanner tous les fichiers dont les extensions commencent par D, comme `DOC`, `DOT` ou `DAT`, saisissez `D*`.

Pour le scan manuel, le scan programmé et le scan immédiat, utilisez un point d'interrogation (?) ou un astérisque (*) comme caractère générique.

Appliquer les paramètres d'exclusion à tous les types de scan

OfficeScan permet de configurer les paramètres d'exclusion pour un type de scan particulier, puis d'appliquer ces mêmes paramètres à tous les autres types de scan. Par exemple :

Le 1er janvier, Chris, administrateur OfficeScan, a découvert qu'il existait un grand nombre de fichiers `JPG` sur les ordinateurs clients et que ces fichiers ne présentaient pas de menaces de sécurité. Chris a ajouté `JPG` à la liste d'exclusion de fichiers pour le scan manuel et appliqué ce paramètre à tous les types de scan. Le scan en temps réel, le scan

immédiat et le scan programmé sont maintenant configurés pour ignorer le scan des fichiers `.jpg`.

Une semaine plus tard, Chris a retiré `JPG` de la liste d'exclusion pour le scan en temps réel mais n'a pas appliqué les paramètres d'exclusions à tous les types de scan. Les fichiers `JPG` seront désormais scannés mais seulement lors du scan en temps réel.

Actions de scan

Spécifiez l'action qu'OfficeScan effectue lorsqu'un type de scan particulier détecte un risque de sécurité. OfficeScan dispose d'un ensemble d'actions de scan différent pour les virus/programmes malveillants et les spywares/graywares.

Actions de scan antivirus/programmes malveillants

L'action de scan entreprise par OfficeScan dépend du type de virus/programme malveillant et du type de scan qui a détecté le virus/programme malveillant. Par exemple, lorsqu'OfficeScan détecte un cheval de Troie (virus/programme malveillant) lors du scan manuel (type de scan), il nettoie (action) le fichier infecté.

Pour plus d'informations sur les différents types de virus/programmes malveillants, reportez-vous à *Virus et programmes malveillants à la page 6-2*

Voici la liste des actions qu'OfficeScan peut effectuer pour lutter contre les virus/programmes malveillants :

TABLEAU 6-10. Actions de scan antivirus/programmes malveillants

ACTION	DESCRIPTION
Supprimer	OfficeScan supprime le fichier infecté.

ACTION	DESCRIPTION
Quarantaine	OfficeScan renomme puis déplace le fichier infecté vers un répertoire de quarantaine temporaire sur l'ordinateur client dans <*Dossier d'installation du client*>`\Suspect`. Le client OfficeScan envoie ensuite les fichiers en quarantaine vers le répertoire de quarantaine désigné. Voir *Répertoire de quarantaine à la page 6-40* pour obtenir des informations détaillées. Le répertoire de quarantaine par défaut se trouve sur le serveur OfficeScan, sous <*Dossier d'installation du serveur*>`\PCCSRV\Virus`. OfficeScan chiffre les fichiers en quarantaine envoyés à ce répertoire. Si vous devez restaurer un fichier mis en quarantaine, utilisez l'outil VSEncrypt. Pour plus d'informations sur l'utilisation de cet outil, consultez *Server Tuner à la page 12-48*.
Nettoyer	OfficeScan nettoie le fichier infecté avant d'autoriser l'accès complet au fichier. Si le fichier n'est pas nettoyable, OfficeScan effectue une seconde action qui peut être l'une des actions suivantes : Mettre en quarantaine, Supprimer, Renommer et Ignorer. Pour configurer la deuxième action, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux**. Cliquez sur l'onglet **Paramètres** > **Paramètres de scan** > **{Type de scan}** > **Action**. Cette action peut effectuée sur tous les types de programmes malveillants, à l'exception des virus/programmes malveillants probables.
Renommer	OfficeScan remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier renommé. Ils peuvent l'ouvrir s'ils associent le fichier à une application déterminée. Le virus/programme malveillant peut s'exécuter lors de l'ouverture du fichier infecté renommé.
Ignorer	OfficeScan ne peut utiliser cette action de scan que lorsqu'il détecte un type de virus donné, lors du scan manuel, du scan programmé et du scan immédiat. OfficeScan ne peut pas utiliser cette action de scan lors du scan en temps réel car l'absence d'action lorsque une tentative d'ouverture ou d'exécution d'un fichier infecté est détectée permettra au virus/programme malveillant de s'exécuter. Toutes les autres actions de scan peuvent être utilisées lors du scan en temps réel.

ACTION	DESCRIPTION
Refuser l'accès	Cette action de scan ne peut être effectuée que pendant un scan en temps réel. Lorsqu'OfficeScan détecte une tentative d'ouverture ou d'exécution d'un fichier infecté, il bloque immédiatement l'opération. Les utilisateurs peuvent supprimer manuellement le fichier infecté.

Utiliser ActiveAction

À chaque type de virus/programme malveillant correspond une action de scan différente. Pour personnaliser une action de scan, vous devez avoir les connaissances nécessaires sur les virus et programmes malveillants. Cette tâche peut s'avérer fastidieuse. OfficeScan utilise ActiveAction pour pallier à ces problèmes.

ActiveAction est un ensemble d'actions de scan pré-configurées, destinées à lutter contre les virus et les programmes malveillants. Si les actions de scan ne vous sont pas familières ou si vous ignorez quelle action est la mieux adaptée à tel ou tel type de virus ou programme malveillant, l'utilisation de l'outil ActiveAction est recommandée.

ActiveAction offre les avantages suivants :

- ActiveAction applique les actions de scan recommandées par Trend Micro. Vous ne perdez plus votre temps à configurer vous-même les actions de scan.
- Les créateurs de virus et programmes malveillants modifient en permanence la manière dont leurs virus attaquent les ordinateurs. Les paramètres d'ActiveAction sont mis à jour pour assurer une protection contre les menaces et les méthodes d'attaques les plus récentes des virus et programmes malveillants.

Remarque

ActiveAction n'est pas disponible pour le scan anti-spywares/graywares.

Le tableau suivant illustre comment ActiveAction traite chaque type de virus/programme malveillant :

TABLEAU 6-11. Actions de scan recommandées par Trend Micro contre les virus et les programmes malveillants

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ/ SCAN IMMÉDIAT	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Canular	Quarantaine	Supprimer	Quarantaine	Supprimer
cheval de Troie	Quarantaine	Supprimer	Quarantaine	Supprimer
Virus	Nettoyer	Quarantaine	Nettoyer	Quarantaine
Virus de test	Refuser l'accès	N/A	N/A	N/A
Utilitaire de compression	Quarantaine	N/A	Quarantaine	N/A
Autres	Nettoyer	Quarantaine	Nettoyer	Quarantaine
Virus/programmes malveillants probables	Refuser l'accès ou action configurée par l'utilisateur	N/A	Ignorer ou action configurée par l'utilisateur	N/A

Pour les virus et programmes malveillants potentiels, l'action par défaut est « Refuser l'accès » pendant le scan en temps réel et « Ignorer » pendant le scan manuel, le scan programmé et le scan immédiat. S'il ne s'agit pas des actions que vous souhaitez effectuer, vous pouvez les modifier par Mettre en quarantaine, Supprimer ou Renommer.

Utilisez la même action pour tous les types de virus/programmes malveillants

Sélectionnez cette option si vous souhaitez que la même action soit entreprise sur tous les types de virus/programmes malveillants, à l'exception de ceux qui sont potentiels. Si vous choisissez «Nettoyer» comme première action, sélectionnez une seconde action qu'OfficeScan doit effectuer si le nettoyage échoue. Si la première action n'est pas «Nettoyer», aucune seconde action n'est configurable.

Si la première action que vous choisissez est « Nettoyer », OfficeScan exécute la deuxième action lorsqu'il détecte des virus/programmes malveillants potentiels.

Utilisez une action spécifique pour chaque type de virus/programme malveillant

Sélectionner manuellement une action de scan pour chaque type de virus/programme malveillant.

Pour tous les types de virus/programmes malveillants, à l'exception de ceux qui sont potentiels, toutes les actions de scan sont disponibles. Si vous choisissez «Nettoyer» comme première action, sélectionnez une seconde action qu'OfficeScan doit effectuer si le nettoyage échoue. Si la première action n'est pas «Nettoyer», aucune seconde action n'est configurable.

Pour les virus et programmes malveillants potentiels, toutes les actions de scan sont disponibles, à l'exception de « Nettoyer ».

Répertoire de quarantaine

Si l'action concernant un fichier infecté est « Mettre en quarantaine », le client OfficeScan encode le fichier et le déplace dans un dossier de quarantaine temporaire situé dans <*Dossier d'installation du client*>\SUSPECT, puis envoie le fichier vers le répertoire de quarantaine désigné.

Remarque

Vous pouvez restaurer des fichiers encodés en quarantaine si vous devez y accéder par la suite. Pour obtenir des informations détaillées, voir *Restauration des fichiers chiffrés à la page 6-44*.

Acceptez le répertoire de quarantaine par défaut, qui se trouve sur l'ordinateur du serveur OfficeScan. Le répertoire est au format URL. Il contient le nom d'hôte du serveur ainsi que l'adresse IP.

- Si le serveur gère simultanément des clients IPv4 et IPv6, utilisez le nom d'hôte de façon à ce que tous les clients puissent envoyer des fichiers mis en quarantaine vers le serveur.

- Si le serveur dispose uniquement d'une adresse IPv4 ou qu'il est identifié par celle-ci, seuls les clients IPv4 purs et les clients double pile peuvent envoyer des fichiers mis en quarantaine vers le serveur.
- Si le serveur dispose uniquement d'une adresse IPv6 ou qu'il est identifié par celle-ci, seuls les clients IPv6 purs et les clients double pile peuvent envoyer des fichiers mis en quarantaine vers le serveur.

Vous pouvez également définir un autre répertoire de quarantaine en saisissant l'emplacement au format URL, chemin UNC ou chemin de fichier absolu. Il convient que les clients aient la possibilité de se connecter à ce répertoire alternatif. Par exemple, le répertoire alternatif doit avoir une adresse IPv6 s'il est susceptible de recevoir des fichiers mis en quarantaine de clients double-pile et de clients IPv6 purs. Trend Micro vous recommande de concevoir un répertoire double-pile alternatif, qui sera identifié par son nom d'hôte et pour lequel vous utiliserez le chemin UNC lorsque vous le saisirez.

Reportez-vous au tableau suivant pour obtenir de l'aide sur l'utilisation d'une URL, d'un chemin UNC ou d'un chemin de fichier absolu :

TABLEAU 6-12. Répertoire de quarantaine

RÉPERTOIRE DE QUARANTAINE	FORMAT ACCEPTÉ	EXEMPLE	REMARQUES
Répertoire installé sur l'ordinateur connecté au serveur OfficeScan	URL	`http://<osceserver>`	Il s'agit du répertoire par défaut. Configurez les paramètres de ce répertoire, comme la taille du dossier de quarantaine. Pour obtenir des informations détaillées, voir *Gestionnaire de quarantaine à la page 12-47*.
	Chemin UNC	`\\<osceserver>\ofcscan\Virus`	

RÉPERTOIRE DE QUARANTAINE	FORMAT ACCEPTÉ	EXEMPLE	REMARQUES
Un répertoire sur un autre ordinateur serveur OfficeScan (si vous avez d'autres serveurs OfficeScan sur votre réseau)	URL	`http://<osceserver2>`	Vérifiez que les clients peuvent se connecter à ce répertoire. Si vous spécifiez un répertoire non valide, le client OfficeScan conserve les fichiers en quarantaine dans le dossier SUSPECT jusqu'à ce que vous spécifiiez un répertoire de quarantaine valide. Dans les journaux de virus/programmes malveillants du serveur, le résultat de scan est «Impossible d'envoyer le fichier en quarantaine vers le dossier de quarantaine spécifié». Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe «Tous» et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe.
	Chemin UNC	`\\<osceserver2>\ofcscan\Virus`	
Autre ordinateur du réseau	Chemin UNC	`\\<computer_name>\temp`	
Autre répertoire installé sur le client OfficeScan	Chemin de fichier absolu	`C:\temp`	

Sauvegardez les fichiers avant nettoyage

Si OfficeScan est configuré pour nettoyer un fichier infecté, il peut commencer par le sauvegarder. Ceci vous permet de restaurer le fichier si vous devez y accéder par la suite. OfficeScan encode le fichier de sauvegarde pour empêcher son ouverture, puis le stocke dans le dossier <*Dossier d'installation du client*>`\Backup`.

Pour restaurer des fichiers de sauvegarde encodés, reportez-vous à *Restauration des fichiers chiffrés à la page 6-44*.

Damage Cleanup Services

Damage Cleanup Services débarrasse les ordinateurs des virus basés sur fichiers et des virus de réseau, ainsi que des résidus de virus et de vers (chevaux de Troie, entrées de registre et fichiers viraux).

Selon le type de scan utilisé, le client déclenche Damage Cleanup Services avant ou après la détection de virus et programmes malveillants.

- Lorsque le scan est de type manuel, programmé ou immédiat, le client OfficeScan active d'abord Damage Cleanup Services, puis procède à la détection des virus et des programmes malveillants. Au cours de la détection de virus et des programmes malveillants, le client est susceptible de déclencher à nouveau Damage Cleanup Services s'il doit procéder à un nettoyage.
- Pendant un scan en temps réel, le client OfficeScan procède tout d'abord à la détection de virus et programmes malveillants, puis déclenche Damage Cleanup Services s'il doit procéder à un nettoyage.

Vous pouvez sélectionner le type de nettoyage effectué par Damage Cleanup Services :

- **Nettoyage standard** : le client OfficeScan exécute l'une des actions suivantes au cours du nettoyage standard :
  - Détecte et supprime les chevaux de Troie actifs
  - Élimine les processus créés par les chevaux de Troie
  - Répare les fichiers système modifiés par les chevaux de Troie
  - Supprime les fichiers et les applications laissés par les chevaux de Troie
- **Nettoyage avancé**: Outre les actions de nettoyage standard, le client OfficeScan interrompt les activités de rogueware, connu également sous le nom de « FakeAV ». Le client OfficeScan utilise aussi les règles de nettoyage avancé afin de détecter et d'arrêter proactivement les applications qui présentent un comportement FakeAV.

Remarque

Tout en assurant une protection proactive, le nettoyage avancé génère également un nombre élevé de faux-positifs.

Damage Cleanup Services ne procède pas au nettoyage des virus et programmes malveillants potentiels, sauf si vous sélectionnez l'option **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté**. Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**. Par exemple, si le client OfficeScan détecte un virus ou un programme malveillant potentiel au cours d'un scan en temps réel et que l'action est Mettre en quarantaine, le client OfficeScan met tout

d'abord le fichier infecté en quarantaine, puis procède au nettoyage si nécessaire. Le type de nettoyage (standard ou avancé) dépend de l'option que vous avez choisie.

Afficher un message de notification lorsqu'un virus/programme malveillant est détecté

Quand OfficeScan détecte un virus/programme malveillant au cours d'un scan en temps réel et d'un scan programmé, il peut afficher un message de notification pour informer l'utilisateur de la détection.

Pour modifier le message de notification, accédez à l'onglet **Virus/Programme malveillant** dans **Notifications** > **Notifications aux utilisateurs clients**.

Afficher un message de notification lorsqu'un virus/programme malveillant potentiel est détecté

Quand OfficeScan détecte un virus/programme malveillant potentiel au cours d'un scan en temps réel et d'un scan programmé, il peut afficher un message de notification pour informer l'utilisateur de la détection.

Pour modifier le message de notification, accédez à l'onglet **Virus/Programme malveillant** dans **Notifications** > **Notifications aux utilisateurs clients**.

Restauration des fichiers chiffrés

Pour empêcher son ouverture, OfficeScan encode un fichier infecté dans les cas suivants :

- Avant de placer un fichier en quarantaine
- Lors de la sauvegarde d'un fichier avant de le nettoyer

OfficeScan fournit un outil qui déchiffre, puis restaure le fichier si vous devez absolument extraire les informations qu'il contient. OfficeScan peut déchiffrer, puis restaurer les fichiers suivants :

TABLEAU 6-13. Fichiers qu'OfficeScan peut déchiffrer et restaurer

FICHIER	DESCRIPTION
Fichiers placés en quarantaine sur l'ordinateur client	Ces fichiers se trouvent dans le dossier <*Dossier d'installation du client*>`\SUSPECT\Backup` et sont purgés automatiquement après 7 jours. Ces fichiers sont également téléchargés dans le répertoire de quarantaine désigné sur le serveur OfficeScan.
Fichiers placés en quarantaine dans le répertoire de quarantaine désigné	Par défaut, ce répertoire se trouve sur l'ordinateur du serveur OfficeScan. Pour obtenir des informations détaillées, voir *Répertoire de quarantaine à la page 6-40*.
Fichiers chiffrés sauvegardés	Il s'agit de la sauvegarde des fichiers infectés qu'OfficeScan a réussi à nettoyer. Ces fichiers se trouvent dans `<Dossier d'installation du client>\Backup`. Pour restaurer ces fichiers, les utilisateurs doivent les déplacer dans `<Dossier d'installation du client>\SUSPECT\Backup`. OfficeScan ne sauvegarde et ne chiffre les fichiers avant de les nettoyer que si vous sélectionnez **Sauvegarder les fichiers détectés avant nettoyage** dans **Ordinateurs en réseau** > **Paramètres clients généraux>Paramètres** > **Paramètres de scan** > **{Type de scan}** > **onglet Action**.

AVERTISSEMENT!

Lorsque vous restaurez un fichier infecté, le virus/programme malveillant qu'il contient peut se propager à d'autres fichiers ou ordinateurs. Avant de restaurer le fichier, isolez l'ordinateur infecté et déplacez les fichiers importants de cet ordinateur vers un emplacement de sauvegarde.

Décryptage et restauration des fichiers

Tâche

- Si le fichier se trouve sur l'ordinateur client OfficeScan :
  a. Ouvrez une invite de commande et accédez au <*Dossier d'installation du client*>.
  b. Exécutez `VSEncode.exe` en saisissant :

```
VSEncode.exe /u
```

Ce paramètre ouvre un écran contenant la liste des fichiers qui se trouvent sous `<Dossier d'installation du client>\SUSPECT\Backup`.

c. Sélectionnez un fichier à restaurer et cliquez sur **Restaurer**. L'outil ne peut restaurer qu'un seul fichier à la fois.

d. Dans l'écran qui s'affiche, indiquez le dossier dans lequel vous voulez restaurer le fichier.

e. Cliquez sur **OK**. Le fichier est restauré dans le dossier spécifié.

Remarque

Il se peut qu'OfficeScan scanne de nouveau le fichier et le considère comme infecté dès sa restauration. Pour éviter qu'il ne soit scanné, ajoutez-le à la liste d'exclusion de scan. Voir *Exclusions de scan à la page 6-31* pour obtenir des informations détaillées.

f. Cliquez sur **Fermer** lorsque vous avez terminé de restaurer des fichiers.

- Si le fichier se trouve sur le serveur OfficeScan ou dans un répertoire de quarantaine personnalisé :

a. Si le fichier se trouve sur l'ordinateur du serveur OfficeScan, ouvrez une invite de commande et accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\VSEncrypt`.

Si le fichier se trouve dans un répertoire de quarantaine personnalisé, accédez à `<Dossier d'installation du serveur>\PCCSRV\Admin\Utility` et copiez le dossier `VSEncrypt` sur l'ordinateur où se trouve le répertoire de quarantaine personnalisé.

b. Créez un fichier texte, puis saisissez le chemin d'accès complet des fichiers que vous souhaitez chiffrer ou déchiffrer.

À titre d'exemple, vous pouvez saisir le chemin d'accès `C:\Mes documents\Reports, \*.* dans le fichier texte pour restaurer tous les fichiers contenus dans C:\Mes documents\Reports`.

Les fichiers placés en quarantaine sur l'ordinateur du serveur OfficeScan se trouvent sous `<Dossier d'installation du serveur>\PCCSRV\Virus`.

c. Enregistrez le fichier texte avec une extension `INI` ou `TXT`. Par exemple, enregistrez-le sous `ForEncryption.ini` sur le lecteur `C:` C:.

d. Ouvrez une fenêtre d'invite et naviguez vers le répertoire dans lequel se trouve le dossier `VSEncrypt`.

e. Exécutez `VSEncode.exe` en saisissant :

```
VSEncode.exe /d /i <emplacement du fichier INI ou TXT>
```

Où :

`<emplacement du fichier INI ou TXT>` est le chemin du fichier `INI` ou `TXT` que vous avez créé (par exemple, `C:\ForEncryption.ini`).

f. Utilisez les autres paramètres pour lancer diverses commandes.

TABLEAU 6-14. Paramètres de restauration

PARAMÈTRE	DESCRIPTION
Aucun (aucun paramètre)	Chiffrer les fichiers
/d	Décoder les fichiers
/debug	Créez un journal de débogage et enregistrez-le sur l'ordinateur. Sur l'ordinateur client OfficeScan, le journal de débogage `VSEncrypt.log` est créé dans le `<Dossier d'installation du client>`.
/o	Remplacer un fichier encodé ou décodé s'il existe déjà
/f <nom du fichier>	Encoder ou décoder un seul fichier
/nr	Ne pas restaurer le nom de fichier original
/v	Afficher des informations concernant l'outil
/u	Lancer l'interface utilisateur de l'outil
/r <Dossier de destination>	Dossier dans lequel un fichier sera restauré

PARAMÈTRE	DESCRIPTION
/s <Nom de fichier original>	Nom du fichier chiffré original

Par exemple, saisissez la commande `VSEncode [/d] [/debug]` pour déchiffrer les fichiers du dossier `Suspect` et créer un journal de débogage. Lorsque vous chiffrez ou déchiffrez un fichier, OfficeScan crée le fichier chiffré ou déchiffré dans le même dossier que le fichier source. Avant de déchiffrer ou de chiffrer un fichier, assurez-vous qu'il n'est pas verrouillé.

Actions de scan anti-spywares/graywares

L'action de scan qu'OfficeScan effectue dépend du type de scan qui a détecté le spyware/grayware. Si des actions spécifiques peuvent être configurées pour chaque type de virus/programme malveillant, une seule action peut l'être pour tous les types de spyware/grayware (pour plus d'informations sur les différents types de spyware/grayware, consultez *Spywares et graywares à la page 6-4*). Par exemple, lorsqu'OfficeScan détecte un type de spyware/grayware lors d'un scan manuel (type de scan), il nettoie (action) les ressources système affectées.

Voici la liste des actions qu'OfficeScan peut effectuer pour lutter contre les graywares/graywares :

TABLEAU 6-15. Actions de scan anti-spywares/graywares

ACTION	DESCRIPTION
Nettoyer	OfficeScan met fin aux processus ou supprime les registres, fichiers, cookies et raccourcis. Après avoir nettoyé des spywares/graywares, les clients OfficeScan sauvegardent les données les concernant. Vous pouvez restaurer celles-ci si vous estimez l'accès aux spywares/graywares sécurisé. Voir *Restauration des spywares/graywares à la page 6-51* pour obtenir des informations détaillées.

ACTION	DESCRIPTION
Ignorer	OfficeScan n'effectue aucune action sur les composants de spyware/grayware détectés mais consigne la détection de spyware/grayware dans les journaux. Cette action n'est possible que lors du scan manuel, du scan programmé et du scan immédiat. Lors du scan en temps réel, l'action est «Refuser l'accès». OfficeScan n'effectue aucune action si le spyware/grayware détecté fait partie de la liste approuvée. Voir *Liste des spywares/graywares approuvés à la page 6-49* pour obtenir des informations détaillées.
Refuser l'accès	OfficeScan refuse l'accès (copie, ouverture) aux composants de spyware/grayware détectés. Cette action ne peut être effectuée que lors d'un scan en temps réel. Lors d'un scan manuel, d'un scan programmé et d'un scan immédiat, l'action est «Ignorer».

Afficher un message de notification lorsqu'un spyware/grayware est détecté

Lorsque OfficeScan détecte un spyware/grayware au cours d'un scan en temps réel et d'un scan programmé, il peut afficher un message de notification pour informer l'utilisateur de la détection.

Pour modifier le message de notification, accédez à **Notifications** > **Notifications aux utilisateurs clients** et cliquez sur l'onglet **Spywares/graywares**.

Liste des spywares/graywares approuvés

OfficeScan fournit une liste des spywares/graywares «approuvés», qui contient les fichiers ou les applications que vous ne souhaitez pas voir considérés comme des spywares ou des graywares. Lorsqu'un spyware/grayware particulier est détecté lors d'un scan, OfficeScan vérifie la liste des spywares/graywares approuvés et n'effectue aucune action si une correspondance est trouvée dans cette liste.

Appliquez la liste des spywares/graywares approuvés à un ou plusieurs clients et domaines, ou à tous les clients que le serveur gère. La liste des spywares/graywares approuvés s'applique à tous les types de scan, ce qui signifie que la même liste approuvée sera utilisée lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat.

Ajout de spywares/graywares détectés à la liste approuvée.

Tâche

1. Accédez à l'un des emplacements suivants :
   - **Ordinateurs en réseau** > **Paramètres clients généraux**
   - **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité**
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Journaux** > **Journaux de spywares/graywares** ou **Afficher journaux** > **Journaux de spywares/graywares**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Sélectionnez les journaux et cliquez sur **Ajouter à la liste approuvée**.
6. Appliquez les spywares/graywares approuvés uniquement aux ordinateurs clients sélectionnés ou à certains domaines.
7. Cliquez sur **Enregistrer**. Les clients sélectionnés appliquent les paramètres et le serveur OfficeScan ajoute le spyware/grayware à la liste approuvée qui se trouve dans **Ordinateurs en réseau** > **Gestion des clients >Paramètres** > **Liste des spywares/graywares approuvés**.

Remarque

OfficeScan peut ajouter un maximum de 1024 spywares/graywares à la liste des spywares/graywares approuvés.

Gestion de la liste des spywares/graywares approuvés

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

3. Cliquez sur **Paramètres** > **Liste des spywares/graywares approuvés**.

4. Dans le tableau **Noms des spywares/graywares**, sélectionnez un nom de spyware/grayware. Pour sélectionner plusieurs noms, maintenez enfoncée la touche **Ctrl** lors de la sélection.

   - Vous pouvez également entrer un mot clé dans le champ **Rechercher** et cliquer sur **Rechercher**. OfficeScan actualise le tableau avec les noms correspondant au mot clé.

5. Cliquez sur **Ajouter**.

   Les noms se déplacent dans le tableau **Liste approuvée**.

6. Pour supprimer les noms dans la liste des spywares/graywares approuvés, sélectionnez les noms et cliquez sur **Supprimer**. Pour sélectionner plusieurs noms, maintenez enfoncée la touche **Ctrl** lors de la sélection.

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Restauration des spywares/graywares

Après avoir nettoyé les spywares/graywares, les clients OfficeScan sauvegardent les données des spywares/graywares. Demandez aux clients en ligne de restaurer les données sauvegardées si vous considérez que les données sont inoffensives. Sélectionnez les données de spyware/grayware à restaurer en fonction de l'heure de sauvegarde.

Remarque

Les utilisateurs clients OfficeScan ne peuvent pas lancer une restauration de spywares/graywares et ne sont pas avertis sur les données de sauvegarde que le client a pu restaurer.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence du client, ouvrez un domaine, puis sélectionnez un client.

   Remarque

   Un seul client à la fois peut procéder à une restauration de spywares/graywares.

3. Cliquez sur **Tâches** > **Restauration de spywares/graywares**.
4. Pour afficher les éléments à restaurer pour chaque segment de données, cliquez sur **Afficher**.

   Un nouvel écran s'affiche. Cliquez sur **Précédent** pour revenir à l'écran précédent.
5. Sélectionnez les segments de données que vous souhaitez restaurer.
6. Cliquez sur **Restaurer**.

   OfficeScan vous indique l'état de la restauration. Consultez les journaux de restauration des spywares/graywares pour obtenir un rapport complet. Voir *Affichage des journaux de restauration de spywares/graywares à la page 6-97* pour obtenir des informations détaillées.

Privilèges et autres paramètres de scan

Les utilisateurs ayant des privilèges de scan ont davantage de contrôle sur la manière dont les fichiers de leur ordinateur sont scannés. Les privilèges de scan permettent aux utilisateurs ou aux clients OfficeScan d'effectuer les tâches suivantes :

- Les utilisateurs peuvent configurer les paramètres de scan manuel, de scan programmé et de scan en temps réel. Pour obtenir des informations détaillées, voir *Privilèges de type de scan à la page 6-53*.
- Les utilisateurs peuvent différer, arrêter ou annuler un scan programmé. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres de scan programmé à la page 6-56*.
- Les utilisateurs peuvent activer le scan de la messagerie Microsoft Outlook et POP3 pour détecter des virus/programmes malveillants dans les messages. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres du scan de courrier à la page 6-62*.
- Le client OfficeScan peut utiliser les paramètres du cache pour améliorer ses performances de scan. Pour obtenir des informations détaillées, voir *Paramètres du cache pour les scans à la page 6-65*.

Privilèges de type de scan

Permet aux utilisateurs de configurer leurs propres paramètres de scan manuel, de scan en temps réel et de scan programmé

Autorisation de privilèges de type de scan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges de scan**.
5. Sélectionnez les types de scan que les utilisateurs sont autorisés à configurer.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Configuration des paramètres de scan pour les ordinateurs clients OfficeScan

Tâche

1. Cliquez avec le bouton droit de la souris sur l'icône du client OfficeScan dans la barre d'état système et sélectionnez **Console OfficeScan**.
2. Cliquez sur **Paramètres** > **{Type de scan}**.

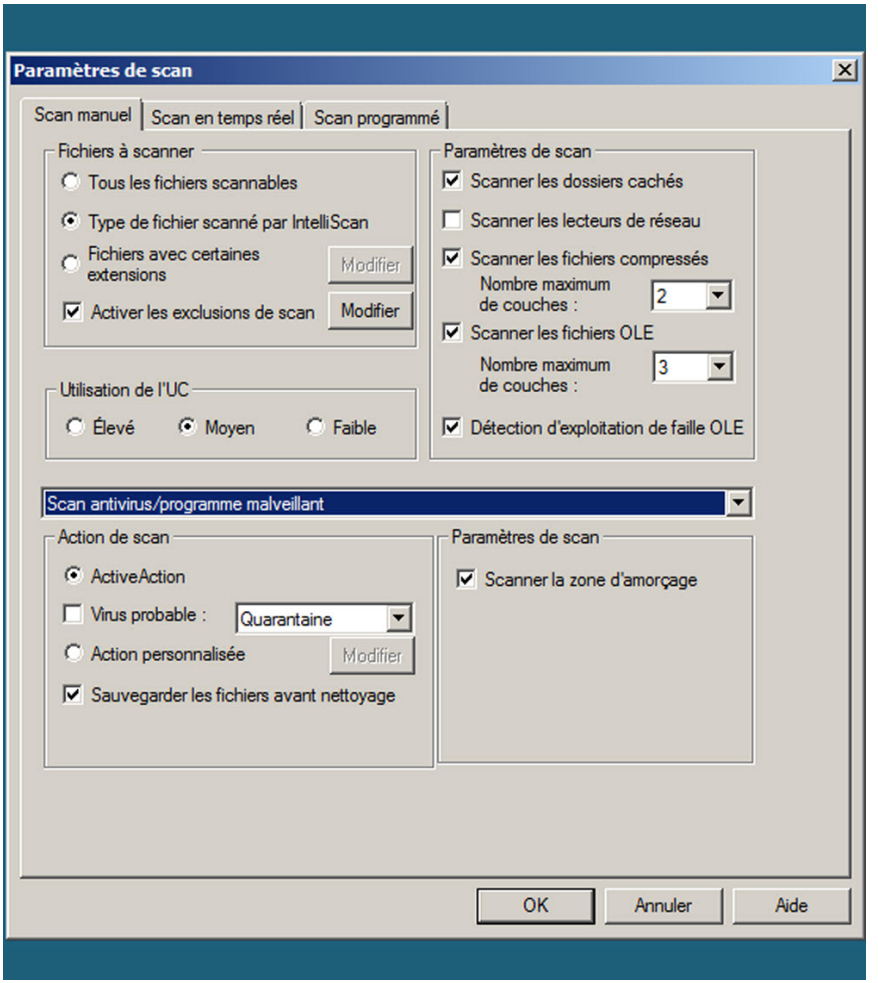


FIGURE 6-1. Paramètres de scan sur la console du client OfficeScan

3. Configurez les paramètres suivants :

   - Paramètres de scan manuel : Fichiers à scanner, Paramètres de scan, Utilisation de l'unité centrale, Exclusions de scan, Actions de scan

- Paramètres de scan en temps réel : Action des utilisateurs sur les fichiers, Fichiers à scanner, Paramètres de scan, Exclusions de scan, Actions de scan
- Paramètres de scan programmé : Programme, Fichiers à scanner, Paramètres de scan, Utilisation de l'unité centrale, Exclusions de scan, Actions de scan

4. Cliquez sur **OK**.

Privilèges et autres paramètres de scan programmé

Si le scan programmé est configuré pour s'exécuter sur le client, les utilisateurs peuvent différer et ignorer/interrompre le scan programmé.

Différer le scan programmé

Les utilisateurs ayant le privilège « Différer le scan programmé » peuvent effectuer les actions suivantes :

- Différer le scan programmé avant qu'il ne débute et définir la durée du report. Le scan programmé ne peut être différé qu'une seule fois.
- Lorsque le scan programmé est en cours, les utilisateurs peuvent l'arrêter et le redémarrer ultérieurement. Les utilisateurs définissent alors la durée devant s'écouler avant le redémarrage du scan. Lorsque le scan reprend, tous les fichiers scannés précédemment sont à nouveau scannés. Le scan programmé peut être arrêté puis redémarré une seule fois.

Remarque

La durée de report minimale/le temps écoulé minimal que les utilisateurs peuvent définir est de 15 minutes. Le maximum est de 12 heures et 45 minutes, que vous pouvez réduire en accédant à **Ordinateurs en réseau** > **Gestion des clients**. Dans la section **Paramètres de scan programmé**, modifiez le paramètre **Différer le scan programmé de__ heures et __ minutes**.

Annuler et arrêter le scan programmé

Ce privilège permet aux utilisateurs d'effectuer les actions suivantes :

- Annuler un scan programmé avant qu'il ne débute
- Arrêter un scan programmé déjà en cours

Notification de privilège de scan programmé

Pour permettre aux utilisateurs de tirer profit des privilèges de scan programmé, rappelez-leur les privilèges que vous leur avez accordés en configurant OfficeScan pour qu'il affiche un message de notification avant l'exécution du scan programmé.

Attribution de privilèges de scan programmé et affichage de la notification de privilège

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de scan programmé**.
5. Sélectionnez les options suivantes :
   - Différer le scan programmé
   - Annuler et arrêter le scan programmé
6. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres de scan programmé**.
7. Sélectionnez **Afficher un message de notification avant le début d'un scan programmé**.

   Lorsque vous activez cette option, un message de notification s'affiche sur l'ordinateur client quelques minutes avant que le scan programmé ne s'exécute. Les utilisateurs sont informés de la programmation de scan (date et heure) et de leurs privilèges de scan programmé, notamment le report, l'annulation ou l'arrêt du scan programmé.

Remarque

Le nombre de minutes peut être configuré. Pour configurer le nombre de minutes, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux**. Dans la section **Paramètres de scan programmé**, modifiez le paramètre **Rappeler le scan programmé aux utilisateurs __ minutes avant qu'il n'exécute le paramètre** .

8. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Report/Annulation et arrêt du scan programmé sur l'ordinateur client

Tâche

- Si le scan programmé n'a pas encore démarré :

  a. Cliquez avec le bouton droit de la souris sur l'icône du client OfficeScan dans la barre d'état système et sélectionnez **Paramètres avancés de scan programmé**.

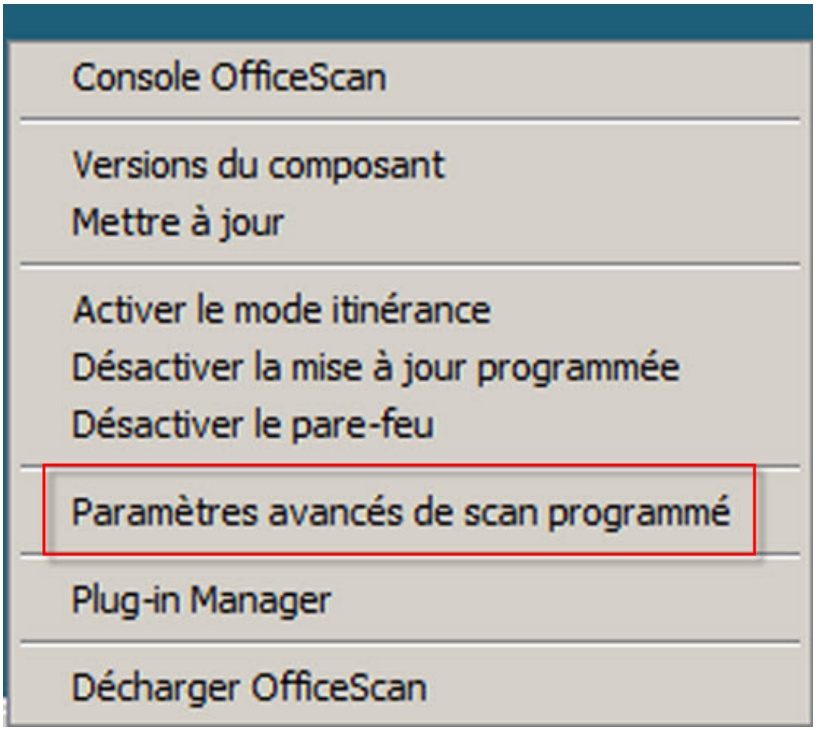


FIGURE 6-2. Option Paramètres avancés de scan programmé

Remarque

Les utilisateurs n'ont pas besoin d'effectuer cette étape si le message de notification est activé et configuré pour s'afficher quelques minutes avant que le scan programmé ne s'exécute. Pour plus de détails sur le message de notification, reportez-vous à *Notification de privilège de scan programmé à la page 6-57*.

b. Dans la fenêtre de notification qui s'affiche, sélectionnez l'une des options suivantes :

- **Différer le scan de __ heures et __ minutes.**
- **Annuler ce scan programmé. Le prochain scan programmé s'exécutera le <date> à <heure>.**

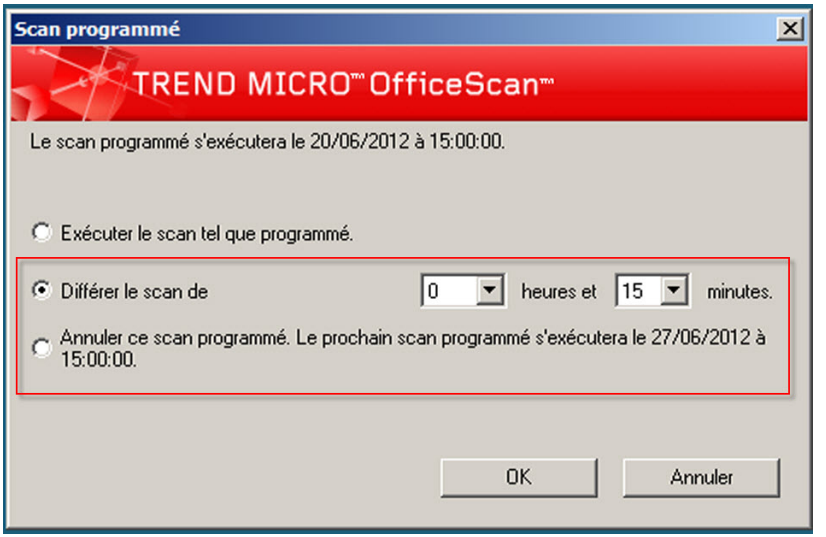


FIGURE 6-3. Privilèges de scan programmé sur l'ordinateur client OfficeScan

- Si le scan programmé est en cours :

  a. Cliquez avec le bouton droit de la souris sur l'icône du client OfficeScan dans la barre d'état système et sélectionnez **Paramètres avancés de scan programmé**.

  b. Dans la fenêtre de notification qui s'affiche, sélectionnez l'une des options suivantes :

     - **Arrêter le scan. Redémarrer le scan après __ heures et __ minutes.**
     - **Arrêter le scan. Le prochain scan programmé s'exécutera le <date> à <heure>.**

FIGURE 6-4. Privilèges de scan programmé sur l'ordinateur client OfficeScan

Privilèges et autres paramètres du scan de courrier

Si les clients disposent des privilèges de scan du courrier, l'onglet **Scan du courrier** s'affiche sur la console du client OfficeScan. L'onglet Scan du courrier du courrier propose deux programmes : scan de messagerie Outlook et scan de messagerie POP3.

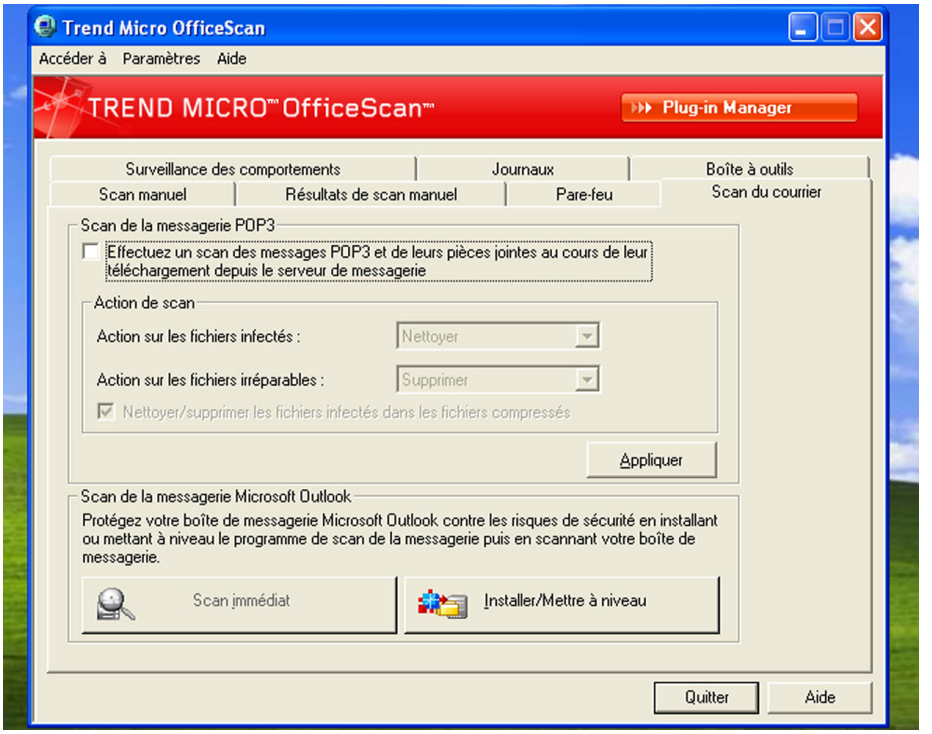

Trend Micro OfficeScan
Accéder à
Paramètres
Aide
TREND MICRO™ OfficeScan™
Plug-in Manager
Surveillance des comportements
Journaux
Boîte à outils
Scan manuel
Résultats de scan manuel
Pare-feu
Scan du courrier
Scan de la messagerie POP3
Effectuez un scan des messages POP3 et de leurs pièces jointes au cours de leur téléchargement depuis le serveur de messagerie
Action de scan
Action sur les fichiers infectés :
Nettoyer
Action sur les fichiers irréparables :
Supprimer
Nettoyer/supprimer les fichiers infectés dans les fichiers compressés
Appliquer
Scan de la messagerie Microsoft Outlook
Protégez votre boîte de messagerie Microsoft Outlook contre les risques de sécurité en installant ou mettant à niveau le programme de scan de la messagerie puis en scannant votre boîte de messagerie.
Scan immédiat
Installer/Mettre à niveau
Quitter
Aide

FIGURE 6-5. Onglet Scan du courrier sur la console du client OfficeScan

Le tableau suivant décrit les programmes de scan de messagerie Outlook et POP3.

TABLEAU 6-16. Programmes de scan de messagerie

DÉTAILS	SCAN DE LA MESSAGERIE OUTLOOK	SCAN DE LA MESSAGERIE POP3
Objet	Scanne les messages de la boîte Microsoft Outlook à la recherche de virus/programmes malveillants.	Scanne les messages de la boîte POP3 à la recherche de virus/ programmes malveillants.
Prérequis	Doit être installé par les utilisateurs à partir de la console client OfficeScan au préalable	• Doit être activé par les administrateurs à partir de la console Web au préalable. **Remarque** Pour activer le scan de la messagerie POP3, voir *Attribution des privilèges du scan de courrier et activation du scan de la messagerie POP3 à la page 6-64*. • Action à effectuer contre les virus et programmes malveillants, à définir à l'aide de la console client OfficeScan, mais pas de la console Web
Types de scan pris en charge	Scan manuel Pour lancer le scan, les utilisateurs doivent cliquer sur **Scan immédiat** à partir de l'onglet **Scan du courrier** de la console client OfficeScan.	Scan en temps réel Le scan s'effectue lors de la récupération des messages électroniques à partir du serveur de messagerie POP3.

DÉTAILS	SCAN DE LA MESSAGERIE OUTLOOK	SCAN DE LA MESSAGERIE POP3
Résultats de scan	• Informations relatives aux risques de sécurité détectés, disponibles après l'exécution du scan. • Résultats de scan non consignés dans l'écran Journaux de la console client OfficeScan • Résultats de scan non envoyés au serveur.	• Informations relatives aux risques de sécurité détectés, disponibles après l'exécution du scan. • Résultats de scan non consignés dans l'écran Journaux de la console client OfficeScan • Résultats de scan non envoyés au serveur.
Autres informations	Aucune	Partage le service proxy d'OfficeScan NT (`TMProxy.exe`) avec la fonction d'évaluation de réputation des sites Web.

Attribution des privilèges du scan de courrier et activation du scan de la messagerie POP3

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges du scan de courrier**.
5. Sélectionnez **Afficher l'onglet Scan du courrier sur la console client**.
6. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres de scan de la messagerie POP3**.
7. Sélectionnez **Scanner la messagerie POP3**.
8. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Paramètres du cache pour les scans

Le client OfficeScan peut générer des fichiers de cache de scan à la demande et de signature numérique pour améliorer les performances du scan. Lors de l'exécution d'un scan à la demande, le client OfficeScan vérifie tout d'abord le fichier de cache de signature numérique, puis le fichier de cache de scan à la demande, pour déterminer les fichiers à exclure du scan. La durée du scan est réduite si de nombreux fichiers sont exclus du scan.

Cache de signature numérique

Le fichier de cache de signature numérique est utilisé lors du scan manuel, du scan programmé et du scan immédiat. Les clients ne scannent pas les fichiers dont les caches ont été ajoutés au fichier de cache de signature numérique.

Le client OfficeScan applique le même Digital Signature Pattern que celui utilisé pour la surveillance des comportements afin de générer le fichier de cache de signature numérique. Le Digital Signature Pattern contient une liste de fichiers que Trend Micro estime fiables et qui sont, par conséquent, exclus des scans.

Remarque

La surveillance des comportements est désactivée pour les plateformes de serveur Windows (prise en charge des plate-formes 64 bits pour Windows XP, 2003, et Vista sans SP1 non disponible). Si le cache de signature numérique est activé, les clients OfficeScan de ces plates-formes téléchargent le Digital Signature Pattern en vue d'une utilisation dans le cache, mais ne téléchargent pas les autres composants de surveillance des comportements.

Les clients génèrent le fichier de cache de signature numérique selon la programmation, configurable à partir de la console Web. Cela permet aux clients de :

- Ajouter le cache aux nouveaux fichiers intégrés au système depuis que le dernier fichier de cache a été généré
- Supprimer le cache des fichiers qui ont été modifiés ou supprimés du système

Pendant le processus de génération du cache, les clients recherchent dans les dossiers suivants les fichiers fiables, puis ajoutent les caches de ces fichiers au fichier de cache de signature numérique :

- `%PROGRAMFILES%`
- `%WINDIR%`

Le processus de génération de cache n'affecte pas les performances de l'ordinateur car les clients consomment des ressources système restreintes au cours de ce processus. Les clients sont également en mesure de reprendre une tâche de génération de cache ayant été interrompue pour un motif quelconque (par exemple, en cas d'extinction de la machine hôte ou de débranchement de l'adaptateur CA d'un ordinateur sans fil).

Mémoire cache du scan à la demande

Le fichier de cache de scan à la demande est utilisé lors du scan manuel, du scan programmé et du scan immédiat. Les clients OfficeScan ne scannent pas les fichiers dont les caches ont été ajoutés au fichier de cache de scan à la demande.

À chaque exécution du scan, le client OfficeScan vérifie les propriétés des fichiers ne présentant pas de menaces. Si un fichier fiable n'a pas été modifié depuis un certain temps (période à configurer), le client OfficeScan ajoute le cache de ce fichier au fichier de cache de scan à la demande. Lors du scan suivant, le fichier n'est pas scanné si son cache n'a pas expiré.

Le cache d'un fichier fiable expire au bout d'un certain nombre de jours (période également à configurer). Lorsque le scan est exécuté pendant ou après l'expiration du cache, le client OfficeScan supprime le cache expiré et scanne le fichier à la recherche de menaces. Si le fichier ne présente aucune menace et qu'aucune modification n'y a été apportée, le cache de ce fichier est de nouveau ajouté au fichier de cache de scan à la demande. Si le fichier ne présente aucune menace, mais qu'une modification y a été

récemment apportée, le cache n'est pas ajouté et ce fichier sera scanné lors du prochain scan.

Un cache de fichier fiable expire pour éviter que des fichiers infectés ne soient exclus des scans, comme l'illustrent les exemples suivants :

- Il est possible qu'un fichier de signatures trop ancien ait considéré un fichier infecté non modifié comme ne présentant aucune menace. S'il n'y a pas d'expiration de cache, le fichier infecté reste dans le système jusqu'à ce qu'il soit modifié et détecté par un scan en temps réel.
- Si un fichier mis en cache a été modifié et que le scan en temps réel ne fonctionne pas depuis la modification du fichier, il est nécessaire que le cache expire pour que le fichier modifié puisse être scanné à la recherche de menaces.

Le nombre de caches ajoutés au fichier de cache de scan à la demande dépend du type de scan et de la cible visée. Par exemple, le nombre de caches peut être réduit si le client OfficeScan scanne uniquement 200 fichiers sur 1 000 d'un ordinateur au cours d'un scan manuel.

Si l'exécution de scans à la demande est fréquente, le fichier de cache de scan à la demande réduit la durée de scan de façon significative. Au cours d'une tâche de scan pour laquelle aucun cache n'a expiré, la durée d'un scan demandant généralement 12 minutes peut être réduite à 1 minute. Pour améliorer les performances, vous pouvez réduire le nombre de jours pendant lequel un fichier n'a pas à être modifié et prolonger la période d'expiration du cache. Étant donné que les fichiers doivent rester inchangés pendant une période relativement courte, vous pouvez ajouter un nombre de caches plus important au fichier de cache. La période d'expiration des caches est également plus longue, ce qui signifie qu'un nombre de fichiers plus important est ignoré au cours de scans.

Si les scans à la demande ne sont que rarement exécutés, vous pouvez désactiver la mémoire cache du scan à la demande car les caches expireront avant l'exécution du prochain scan.

Configuration des paramètres du cache pour les scans

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.

2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres du cache pour les scans**.

5. Configurez les paramètres applicables au cache de signature numérique.

   a. Sélectionnez **Activer le cache de la signature numérique**.

   b. Dans la zone **Générer le cache tous les __ jours**, indiquez la fréquence à laquelle le client génère le cache.

6. Configurez les paramètres applicables au cache de scan à la demande.

   a. Sélectionnez **Activer le cache du Scan à la demande**.

   b. Dans la zone **Ajouter le cache pour les fichiers légitimes qui n'ont pas été modifiés depuis __ jours**, spécifiez le nombre de jours pendant lequel un fichier doit rester inchangé avant qu'il ne soit mis en cache.

   c. Dans la zone **Le cache de tous les fichiers légitimes expire dans __ jours**, indiquez la période maximale en jours pendant laquelle un cache reste dans le fichier de cache.

   Remarque

   Pour éviter que les caches ajoutés au cours d'un scan n'expirent le même jour, les caches expirent de façon aléatoire au cours de la période maximale en jours que vous avez spécifiée. Par exemple, si 500 fichiers sont ajoutés au cache aujourd'hui et que la période maximale spécifiée est de 10 jours, une partie des caches expirera demain, et la majorité d'entre eux, au cours des jours suivants. Au dixième jour, tous les caches restants expireront.

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les

domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Paramètres de scan généraux

Les paramètres de scan généraux peuvent être appliqués aux clients de diverses manières.

- Un paramètre de scan donné peut s'appliquer à tous les clients gérés par le serveur ou uniquement à ceux qui disposent de certains privilèges de scan. Par exemple, si vous configurez la durée du report du scan programmé, seuls les clients disposant du privilège les autorisant à reporter le scan programmé seront concernés par ce paramètre.
- Un paramètre de scan donné peut s'appliquer à tous les types de scan ou à un type particulier. Par exemple, dans le cas d'ordinateurs sur lesquels le serveur OfficeScan et le client OfficeScan ont l'un et l'autre été installés, vous pouvez exclure du scan la base de données du serveur OfficeScan. Cependant, ce paramètre ne s'applique que durant les scans en temps réel.
- Un paramètre de scan donné peut s'appliquer aux recherches de virus/programmes malveillants, aux recherches de spywares/graywares, ou aux deux types de recherche. Le mode d'évaluation, par exemple, ne s'applique qu'aux scans visant à détecter des spywares/graywares.

Configuration des paramètres de scan généraux

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Configurez les paramètres de scan généraux dans chacune des sections disponibles.

- *Section des paramètres de scan à la page 6-70*
- *Section des paramètres de scan programmé à la page 6-76*
- *Section des paramètres de bande passante des journaux de virus/programmes malveillants à la page 6-78*

3. Cliquez sur **Enregistrer**.

Section des paramètres de scan

La section Paramètres de scan des paramètres de scan généraux permet aux administrateurs de configurer ce qui suit :

- *Configurer les paramètres de scan pour les gros fichiers compressés à la page 6-70*
- *Ajouter le scan manuel au menu des raccourcis Windows sur les ordinateurs clients OfficeScan à la page 6-71*
- *Exclure du scan en temps réel la base de données du serveur OfficeScan à la page 6-71*
- *Exclure des scans les dossiers et les fichiers du serveur Microsoft Exchange à la page 6-72*
- *Nettoyer/supprimer les fichiers infectés dans les fichiers compressés à la page 6-72*
- *Activer le mode d'évaluation à la page 6-75*
- *Recherche de cookies à la page 6-76*

Configurer les paramètres de scan pour les gros fichiers compressés

Tous les clients OfficeScan gérés par le serveur vérifient les paramètres suivants lorsqu'ils scannent les fichiers compressés à la recherche de virus/programmes malveillants et de spywares/graywares lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat :

- **Ne pas scanner les fichiers inclus dans le fichier compressé si la taille dépasse __ Mo** : OfficeScan ne scanne pas les fichiers dont la taille dépasse la limite indiquée.

- **Dans un fichier compressé, scanner uniquement les __ premiers fichiers** : Après la décompression d'un fichier compressé, OfficeScan scanne le nombre de fichiers spécifié et ignore les fichiers restants, le cas échéant.

Ajouter le scan manuel au menu des raccourcis Windows sur les ordinateurs clients OfficeScan

Lorsque ce paramètre est activé, tous les clients OfficeScan gérés par le serveur ajoutent une option **Scanner avec le client OfficeScan** au menu de l'Explorateur Windows accessible avec le bouton droit. Lorsque les utilisateurs cliquent avec le bouton droit sur un fichier ou un dossier sur le bureau de Windows ou dans l'Explorateur Windows et sélectionnent l'option, le scan manuel scanne le fichier ou le dossier pour rechercher les virus/programmes malveillants et les spywares/graywares.

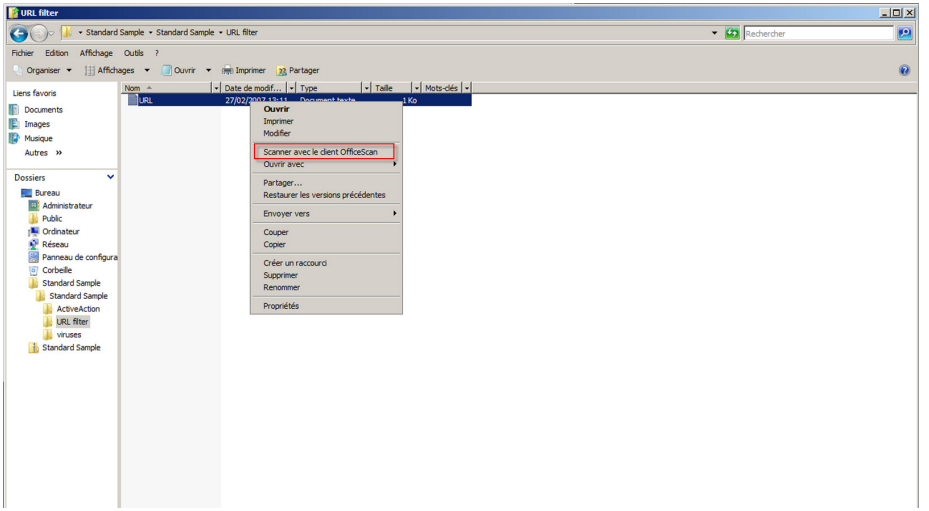


FIGURE 6-6. Option Scanner avec le client OfficeScan

Exclure du scan en temps réel la base de données du serveur OfficeScan

Si le client OfficeScan et le serveur OfficeScan sont installés sur le même ordinateur, le client OfficeScan ne scannera pas la base de données du serveur pour rechercher les virus/programmes malveillants et les spywares/graywares lors du scan en temps réel.

Conseil

Activez ce paramètre pour empêcher toute détérioration de la base de données susceptible de se produire lors du scan.

Exclure des scans les dossiers et les fichiers du serveur Microsoft Exchange

Si le client OfficeScan et un serveur Microsoft Exchange 2000/2003 sont installés sur le même ordinateur, OfficeScan ne scannera pas les dossiers et les fichiers suivants de Microsoft Exchange pour rechercher les virus/programmes malveillants et les spywares/graywares lors du scan manuel, en temps réel, programmé et immédiat.

- Les dossiers suivants qui se trouvent sous `\Exchsrvr\Mailroot\vsi 1` : `Queue`, `PickUp` et `BadMail`
- `.\Exchsrvr\mdbdata`, y compris ces fichiers : `priv1.stm`, `priv1.edb`, `pub1.stm` et `pub1.edb`
- `.\Exchsrvr\Storage Group`

Pour les dossiers de Microsoft Exchange 2007 ou version supérieure, vous devez ajouter manuellement les dossiers à la liste d'exclusion de scan. Pour plus d'informations sur les exclusions de scan, consultez le site Web suivant :

http://technet.microsoft.com/en-us/library/bb332342.aspx

Voir *Exclusions de scan à la page 6-31* pour connaître les étapes de configuration de la liste d'exclusion de scan.

Nettoyer/supprimer les fichiers infectés dans les fichiers compressés

Lorsque tous les clients gérés par le serveur détectent des virus/programmes malveillants dans les fichiers compressés lors du scan manuel, en temps réel, programmé ou immédiat et que les conditions suivantes sont remplies, les clients nettoient ou suppriment les fichiers infectés.

- « Nettoyer » ou « Supprimer » est l'action qu'OfficeScan doit effectuer. Vérifiez l'action qu'entreprend OfficeScan à l'encontre des fichiers infectés en accédant à l'onglet **Ordinateurs en réseau** > **Paramètres clients généraux > Paramètres** > **Paramètres de scan** > **{Type de scan}** > **Action**.

- Activez ce paramètre. Le choix de ce paramétrage est susceptible d'augmenter l'utilisation des ressources de l'ordinateur pendant le scan qui peut, de ce fait, durer plus longtemps. Ceci est dû au fait qu'OfficeScan doit décompresser le fichier compressé, nettoyer/supprimer les fichiers infectés qu'il contient, puis le compresser à nouveau.
- Le format de fichier compressé est pris en charge. OfficeScan ne prend en charge que certains formats de fichiers compressés, parmi lesquels figurent ZIP et Office Open XML, qui utilise les technologies de compression ZIP. Office Open XML est le format par défaut pour les applications Microsoft Office 2007 telles qu'Excel, PowerPoint et Word.

Remarque

Contactez votre service d'assistance pour obtenir une liste complète des formats de fichiers compressés pris en charge.

Par exemple, le scan en temps réel est configuré pour supprimer les fichiers infectés par un virus. Lorsque le scan en temps réel décompresse un fichier compressé nommé `abc.zip` et détecte dans celui-ci un fichier infecté nommé `123.doc` , OfficeScan supprime `123.doc`, puis compresse à nouveau `abc.zip`, qui est désormais accessible en toute sécurité.

Le tableau suivant décrit ce qui se passe lorsque l'une des conditions n'est pas remplie.

TABLEAU 6-17. Scénarios et résultats pour les fichiers compressés

ÉTAT DE « NETTOYER/ SUPPRIMER LES FICHIERS INFECTÉS DANS LES FICHIERS COMPRESSÉS »	ACTION QUE DOIT EFFECTUER OFFICESCAN	FORMAT DE FICHIER COMPRESSÉ	RÉSULTAT
Activé	Nettoyer ou Supprimer	Non pris en charge Exemple : `def.rar` contient un fichier infecté `123.doc`.	OfficeScan chiffre `def.rar`, mais ne nettoie pas, ne supprime pas et n'entreprend aucune autre action à l'encontre de `123.doc`.
Désactivé	Nettoyer ou Supprimer	Pris en charge/Non pris en charge Exemple : `abc.rar` contient un fichier infecté `123.doc`.	OfficeScan ne nettoie pas, ne supprime pas et n'entreprend aucune autre action à l'encontre de `abc.zip` et `123.doc`.

ÉTAT DE « NETTOYER/ SUPPRIMER LES FICHIERS INFECTÉS DANS LES FICHIERS COMPRESSÉS »	ACTION QUE DOIT EFFECTUER OFFICESCAN	FORMAT DE FICHIER COMPRESSÉ	RÉSULTAT
Activé/ Désactivé	Ni Nettoyer ni Supprimer (en d'autres termes, l'une des actions suivantes : Renommer, Mettre en quarantaine, Refuser l'accès ou Ignorer)	Pris en charge/Non pris en charge Exemple : `abc.rar` contient un fichier infecté `123.doc`.	OfficeScan entreprend l'action configurée (Renommer, Mettre en quarantaine, Refuser l'accès ou Ignorer) à l'encontre du fichier `abc.zip` et pas du fichier `123.doc` Si l'action est : **Renommer**: OfficeScan renomme `abc.zip` en `abc.vir`, mais ne renomme pas `123.doc`. **Quarantaine** : OfficeScan met en quarantaine `abc.zip` (`123.doc` et tous les fichiers non infectés sont mis en quarantaine). **Ignorer** : OfficeScan n'entreprend aucune action à l'encontre de `abc.zip` et `123.doc` mais consigne la détection de virus. **Refuser l'accès** : OfficeScan refuse l'accès à `abc.zip` lorsque l'on tente de l'ouvrir (`123.doc` et tous les fichiers non infectés ne peuvent pas être ouverts).

Activer le mode d'évaluation

En mode d'évaluation, tous les clients gérés par le serveur enregistrent dans le journal les spywares/graywares détectés pendant le scan manuel, programmé, en temps réel et immédiat, mais ne nettoient pas les composants des spywares/graywares. Le nettoyage met fin aux processus ou supprime les répertoires, fichiers, cookies et raccourcis.

Le mode d'évaluation de Trend Micro a été conçu pour vous permettre d'évaluer les éléments que Trend Micro détecte comme étant des spywares/graywares avant d'entreprendre une action en fonction de votre évaluation. Par exemple, les spywares/graywares détectés qui ne constituent pas selon vous un risque de sécurité peuvent être ajoutés à la liste des spywares/graywares approuvés.

En mode d'évaluation, OfficeScan effectue les actions de scan suivantes :

- **Ignorer** : pendant le scan manuel, le scan programmé et le scan immédiat
- **Refuser l'accès** : pendant le scan en temps réel

Remarque

Le mode d'évaluation a la priorité sur toute action de scan configurée par l'utilisateur. Par exemple, même si vous choisissez « Nettoyer » comme action lors du scan manuel, « Ignorer » reste l'action de scan lorsque le client est en mode d'évaluation.

Recherche de cookies

Sélectionnez cette option si vous considérez les cookies comme des risques de sécurité potentiels. Lorsqu'elle est sélectionnée, tous les clients gérés par le serveur scannent les cookies pour rechercher des spywares/graywares pendant le scan manuel, programmé, en temps réel et immédiat.

Section des paramètres de scan programmé

Seuls les clients configurés pour exécuter le scan programmé utiliseront les paramètres suivants. Le scan programmé peut rechercher les virus/programmes malveillants et les spywares/graywares.

La section Paramètres de scan programmé des paramètres de scan généraux permet aux administrateurs de configurer ce qui suit :

- *Rappeler le scan programmé aux utilisateurs __ minutes avant qu'il ne débute à la page 6-77*
- *Différer le scan programmé de __ heure(s) et __ minute(s) maximum à la page 6-77*
- *Arrêter automatiquement le scan programmé lorsque le scan dure depuis plus de __ heure(s) et __ minute(s) à la page 6-77*

- *Annuler le scan programmé lorsque l'autonomie de la batterie d'un ordinateur sans fil est inférieure à __ % et que l'adaptateur CA est débranché. à la page 6-78*
- *Reprendre un scan programmé ignoré à la page 6-78*

Rappeler le scan programmé aux utilisateurs __ minutes avant qu'il ne débute

OfficeScan affiche un message de notification quelques minutes avant que le scan ne débute pour rappeler aux utilisateurs la programmation de scan (date et heure) et tous les privilèges de scan programmé que vous leur avez accordés.

Le message de notification peut être activé/désactivé depuis **Ordinateurs en réseau** > **Paramètres clients généraux > Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres (onglet)** > **Paramètres de scan programmé**. S'il est désactivé, aucun rappel ne s'affiche.

Différer le scan programmé de __ heure(s) et __ minute(s) maximum

Seuls les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes :

- Différer le scan programmé avant qu'il ne débute et définir la durée du report.
- Lorsque le scan programmé est en cours, les utilisateurs peuvent l'arrêter et le redémarrer ultérieurement. Les utilisateurs définissent alors la durée devant s'écouler avant le redémarrage du scan. Lorsque le scan reprend, tous les fichiers scannés précédemment sont à nouveau scannés.

  La durée de report maximale/le temps écoulé maximal que les utilisateurs peuvent définir est de 12 heures et 45 minutes. Vous pouvez réduire cette durée en spécifiant le nombre d'heures et/ou de minutes dans les champs prévus à cet effet.

Arrêter automatiquement le scan programmé lorsque le scan dure depuis plus de __ heure(s) et __ minute(s)

OfficeScan arrête le scan lorsque le délai spécifié est dépassé et que le scan n'est pas encore terminé. OfficeScan avertit immédiatement les utilisateurs des risques de sécurité détectés pendant le scan.

Annuler le scan programmé lorsque l'autonomie de la batterie d'un ordinateur sans fil est inférieure à __ % et que l'adaptateur CA est débranché.

OfficeScan annule automatiquement le scan programmé lors de son lancement s'il détecte que l'autonomie de la batterie d'un ordinateur sans fil devient faible et que son adaptateur CA n'est pas raccordé à une source d'alimentation. Si l'autonomie de la batterie est faible mais que l'adaptateur CA est raccordé à une source d'alimentation, le scan se poursuit.

Reprendre un scan programmé ignoré

Lorsqu'un scan programmé n'est pas lancé parce que OfficeScan n'est pas en cours d'exécution au jour et à l'heure prévus, vous pouvez indiquer à quel moment OfficeScan reprendra le scan :

- **à la même heure le jour suivant** : si OfficeScan s'exécute exactement à la même heure le lendemain, le scan reprend.
- **__ minutes après le démarrage de l'ordinateur** : OfficeScan reprend le scan un certain nombre de minutes après que l'utilisateur a mis l'ordinateur sous tension. Le nombre de minutes peut être compris entre 10 et 120.

Remarque

Les utilisateurs peuvent reporter ou ignorer un scan programmé repris si l'administrateur leur a accordé ce privilège. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres de scan programmé à la page 6-56*.

Section des paramètres de bande passante des journaux de virus/programmes malveillants

La section des paramètres de bande passante des journaux de virus/programmes malveillants des paramètres de scan généraux permet aux administrateurs de configurer :

Permettre aux clients OfficeScan de créer une entrée unique dans le journal de virus/programmes malveillants pour les détections récurrentes d'un même virus/programme malveillant en l'espace d'une heure à la page 6-79

Permettre aux clients OfficeScan de créer une entrée unique dans le journal de virus/programmes malveillants pour les détections récurrentes d'un même virus/programme malveillant en l'espace d'une heure

OfficeScan rassemble les entrées des journaux de virus lorsque de multiples infections provenant des mêmes virus/programmes malveillants sont détectées sur une courte période. OfficeScan peut détecter un même virus/programme malveillant à plusieurs reprises. Il remplit alors rapidement le journal de virus/programmes malveillants et sollicite la bande passante du réseau lorsque le client OfficeScan envoie les informations du journal au serveur. L'activation de cette fonctionnalité permet de réduire à la fois le nombre d'entrées de virus/programmes malveillants consignées et la bande passante du réseau que les clients OfficeScan utilisent lorsqu'ils soumettent au serveur des informations du journal de virus.

Notifications sur les risques liés à la sécurité

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que d'autres administrateurs OfficeScan et les utilisateurs du client OfficeScan, des risques liés à la sécurité détectés.

Pour plus de détails sur les notifications envoyées aux administrateurs, voir *Notifications sur les risques liés à la sécurité pour les administrateurs à la page 6-79*.

Pour plus d'informations sur les notifications envoyées aux utilisateurs du client OfficeScan, consultez *Notifications sur les risques liés à la sécurité pour les utilisateurs du client OfficeScan à la page 6-83*.

Notifications sur les risques liés à la sécurité pour les administrateurs

Configurez OfficeScan pour qu'il vous envoie, ainsi qu'aux autres administrateurs OfficeScan, une notification lorsqu'un risque lié à la sécurité est détecté ou uniquement lorsque l'action entreprise contre le risque échoue et que par conséquent, une intervention de votre part s'impose.

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, des détections de risques liés

à la sécurité. Vous pouvez modifier les notifications et configurer des paramètres de notification supplémentaires qui répondent à vos exigences.

Remarque

OfficeScan peut vous envoyer des notifications par courrier électronique, pageur, déroutement SNMP et par le journal des événements de Windows NT. Configurez les paramètres lorsqu'OfficeScan envoie des notifications par le biais de ces chaînes. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 12-32*.

Configuration des notifications sur les risques liés à la sécurité pour les administrateurs

Tâche

1. Accédez à **Notifications** > **Notifications administrateur** > **Notifications standard**.
2. Dans l'onglet **Critères** :
   a. Accédez aux sections **Virus/Programmes malveillants** et **Spywares/ Graywares**.
   b. Déterminez si des notifications doivent être envoyées lorsqu'OfficeScan détecte des virus/programmes malveillants et des spywares/graywares ou uniquement lorsque l'action effectuée sur ces risques de sécurité échoue.
3. Dans l'onglet **Courrier électronique** :
   a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.
   b. Sélectionnez **Activer la notification par courrier électronique**.
   c. Sélectionnez **Envoyer les notifications aux utilisateurs ayant les droits d'accès au domaine de l'arborescence des clients**.

      Vous pouvez utiliser l'administration basée sur les rôles afin de donner aux utilisateurs l'accès au domaine de l'arborescence des clients. Si une anomalie est détectée chez un client OfficeScan appartenant à un domaine spécifique, le

courrier électronique sera envoyé aux adresses électroniques des utilisateurs ayant les autorisations sur ce domaine Pour des exemples, voir le tableau suivant :

TABLEAU 6-18. Domaines et droits d'accès de l'arborescence des clients

DOMAINE DE L'ARBORESCENCE DES CLIENTS	RÔLES AVEC DROITS D'ACCÈS AU DOMAINE	COMPTE UTILISATEUR AVEC LE RÔLE	ADRESSE ÉLECTRONIQUE POUR LE COMPTE UTILISATEUR
Domaine A	Administrateur (intégré)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domaine B	Administrateur (intégré)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un client OfficeScan appartenant au domaine A détecte un virus, le courrier électronique sera envoyé à mary@xyz.com, john@xyz.com, et chris@xyz.com.

Si un client OfficeScan appartenant au domaine B détecte des spywares, le courrier électronique sera envoyé à mary@xyz.com et jane@xyz.com.

Remarque

Si vous activez cette option, tous les utilisateurs ayant les autorisations sur ce domaine doivent avoir des adresses électroniques correspondantes. La notification par courrier électronique ne sera pas envoyée aux utilisateurs qui n'ont pas d'adresse électronique. Les utilisateurs et les adresses électroniques sont configurés à partir de **Administration** > **Comptes utilisateurs**.

d. Sélectionnez **Envoyer les notifications à/aux (l')adresse(s) électronique(s) suivante(s)**, puis saisissez les adresses électroniques.

e. Acceptez ou modifiez l'objet et le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 6-19. Variables de jetons pour les notifications de risques liés à la sécurité

VARIABLE	DESCRIPTION
Détections de virus/programmes malveillants	
%v	Nom du virus/programme malveillant
%s	Ordinateur infecté par un virus/programme malveillant
%i	Adresse IP de l'ordinateur
%c	Adresse MAC de l'ordinateur
%m	Domaine de l'ordinateur
%p	Emplacement du virus/programme malveillant
%y	Date et heure de la détection du virus/programme malveillant
%e	Version du moteur de scan antivirus
%r	Version du fichier de signatures de virus
%a	Action effectuée sur le risque de sécurité
%n	Nom de l'utilisateur connecté à l'ordinateur infecté
Détections de spywares/graywares	
%s	Ordinateur infecté par un spyware/grayware
%i	Adresse IP de l'ordinateur
%m	Domaine de l'ordinateur
%y	Date et heure de la détection du spyware/grayware
%n	Nom de l'utilisateur connecté à l'ordinateur au moment de la détection
%T	Résultat de scan anti-spywares/graywares

4. Dans l'onglet **Pageur** :

a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.

b. Sélectionnez **Activer la notification par pageur**.

c. Saisissez le message.

5. Dans l'onglet **Déroutement SNMP**.

a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.

b. Sélectionnez **Activer la notification par déroutement SNMP**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 6-19 à la page 6-82* pour obtenir des informations détaillées.

6. Dans l'onglet **Journal des événements NT** :

a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.

b. Sélectionnez **Activer la notification via le journal d'événements NT**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 6-19 à la page 6-82* pour obtenir des informations détaillées.

7. Cliquez sur **Enregistrer**.

Notifications sur les risques liés à la sécurité pour les utilisateurs du client OfficeScan

OfficeScan peut afficher des messages de notification sur les ordinateurs du client OfficeScan :

- Tout de suite après, les scan en temps réel et scan programmé détectent les virus/programmes malveillants et les spywares/graywares. Activez le message de notification et modifiez éventuellement son contenu.

- Si le redémarrage d'un ordinateur client est nécessaire pour terminer le nettoyage des fichiers infectés. Pour le scan en temps réel, le message s'affiche après la détection d'un risque de sécurité particulier. Pour le scan manuel, le scan programmé et le scan immédiat, le message s'affiche une seule fois, et uniquement après qu'OfficeScan a fini de scanner toutes les cibles de scan.

Notification aux utilisateurs de détections de virus/programmes malveillants et de spywares/graywares

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan en temps réel** ou **Paramètres** > **Paramètres de scan** > **Paramètres de scan programmé**.
4. Cliquez sur l'onglet Action.
5. Sélectionnez les options suivantes :
   - **Afficher un message de notification sur l'ordinateur client lorsqu'un virus/programme malveillant est détecté**
   - **Afficher un message de notification sur l'ordinateur client lorsqu'un virus/programme malveillant probable est détecté**
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Configuration des notifications de virus/programme malveillant

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.
2. Cliquez sur l'onglet **Virus/programmes malveillants**.
3. Configurez les paramètres de détection.
   a. Choisissez d'afficher une notification pour tous les événements liés aux virus/programmes malveillants ou séparez les notifications en fonction des niveaux de gravité suivants :
      - **Élevé** : Le client OfficeScan n'a pas pu gérer un programme malveillant critique
      - **Moyen**: Le client OfficeScan n'a pas pu gérer un programme malveillant
      - **Faible** : Le client OfficeScan est parvenu à résoudre toutes les menaces
   b. Acceptez ou modifiez les messages par défaut.
4. Pour afficher un message de notification si le virus/programme malveillant provient de l'ordinateur de l'utilisateur client :
   a. Cochez la case sous **Source de l'infection par virus/programmes malveillants**.
   b. Spécifiez un intervalle entre les envois de notification.
   c. Éventuellement, modifiez le message de notification par défaut.

Remarque

Ce message de notification s'affiche uniquement si vous activez le service Windows Messenger. Vérifiez l'état de ce service dans l'écran Services (**Panneau de configuration** > **Outils administrateurs** > **Services** > **Messenger**).

5. Cliquez sur **Enregistrer**.

Configuration des notifications de spyware/grayware

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.
2. Cliquez sur l'onglet **Spyware/Grayware**.
3. Acceptez ou modifiez le message par défaut.
4. Cliquez sur **Enregistrer**.

Notification de redémarrage destinée aux clients afin de terminer le nettoyage des fichiers infectés

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Notification de redémarrage**.
5. Sélectionnez **Afficher un message de notification si l'ordinateur client doit redémarrer pour terminer le nettoyage des fichiers infectés**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les

domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Journaux de risques de sécurité

OfficeScan génère des journaux lorsqu'il détecte des virus/programmes malveillants ou des spywares/graywares, et lorsqu'il restaure des spywares/graywares.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de virus/programmes malveillants

Le client OfficeScan génère des journaux lorsqu'il détecte des virus et programmes malveillants, et les envoie au serveur.

Tâche

1. Accédez à l'un des emplacements suivants :
   - **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité**
   - **Ordinateurs en réseau** > **Gestion des clients**
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Journaux** > **Journaux de virus/programmes malveillants** ou **Afficher journaux** > **Journaux de virus/programmes malveillants**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.

5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date et heure de la détection du virus/programme malveillant
   - Ordinateur infecté
   - Nom du virus/programme malveillant
   - Source de l'infection
   - Fichier infecté
   - Type de scan qui a détecté le virus/programme malveillant
   - Résultats de scan

   Remarque

   Pour plus d'informations sur les résultats de scan, consultez *Résultats de scan antivirus/programmes malveillants à la page 6-88*.

   - adresse IP
   - Adresse MAC
   - Détails des journaux (Cliquez sur **Afficher** pour consulter les détails.)
6. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

   Le fichier CSV contient les informations suivantes :
   - Toutes les informations dans les journaux
   - Nom d'utilisateur connecté à l'ordinateur au moment de la détection

Résultats de scan antivirus/programmes malveillants

Les résultats de scan suivants s'affichent dans les journaux de virus/programmes malveillants :

- **Supprimé**

  - La première action est Supprimer et le fichier infecté a été supprimé.
  - La première action est Nettoyer, mais le nettoyage a échoué. La deuxième action est Supprimer et le fichier infecté a été supprimé.

- **Mis en quarantaine**
  - La première action est Mettre en quarantaine et le fichier infecté a été mis en quarantaine.
  - La première action est Nettoyer, mais le nettoyage a échoué. La deuxième action est Mettre en quarantaine et le fichier infecté a été mis en quarantaine.

- **Nettoyé**

  Un fichier infecté a été nettoyé.

- **Renommé**
  - La première action est Renommer et le fichier infecté a été renommé.
  - La première action est Nettoyer, mais le nettoyage a échoué. La deuxième action est Renommer et le fichier infecté a été renommé.

- **Accès refusé**
  - La première action est Refuser l'accès et l'accès au fichier infecté a été refusé lorsque l'utilisateur a tenté d'ouvrir le fichier.
  - La première action est Nettoyer, mais le nettoyage a échoué. La deuxième action est Refuser l'accès et l'accès au fichier infecté a été refusé lorsque l'utilisateur a tenté d'ouvrir le fichier.
  - Un virus/programme malveillant potentiel a été détecté lors du scan en temps réel.
  - Le scan en temps réel peut interdire l'accès aux fichiers infectés par un virus d'amorce, même si l'action de scan est Nettoyer (première action) et Mettre en quarantaine (deuxième action). Ceci est dû au fait que la tentative de nettoyage d'un virus d'amorce risque d'endommager le Master Boot Record (MBR) de l'ordinateur infecté. lancez le scan manuel de sorte qu'OfficeScan puisse nettoyer ou mettre en quarantaine le fichier.

- **Ignoré**

- La première action est Ignorer. OfficeScan n'a entrepris aucune action à l'encontre de ce fichier.
- La première action est Nettoyer, mais le nettoyage a échoué. La deuxième action est Ignorer. Ainsi, OfficeScan n'a entrepris aucune action à l'encontre du fichier infecté.

- **Un risque de sécurité potentiel a été ignoré**

  Ce résultat de scan ne s'affiche que lorsqu'OfficeScan détecte un «virus/programme malveillant potentiel» lors du scan manuel, du scan programmé et du scan immédiat. Reportez-vous à la page suivante de l'encyclopédie en ligne des virus de Trend Micro pour obtenir des informations sur les virus/programmes malveillants potentiels et sur l'envoi de fichiers suspects à Trend Micro pour analyse.

  http://www.trendmicro.com/vinfo/fr/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn

- **Impossible de nettoyer le fichier ou de le mettre en quarantaine**

  Nettoyer est la première action. Mettre en quarantaine est la seconde action et les deux actions ont échoué.

  Solution : Voir *Impossible de mettre le fichier en quarantaine/Impossible de renommer le fichier à la page 6-90*.

- **Impossible de nettoyer ou supprimer le fichier**

  Nettoyer est la première action. Supprimer est la seconde action et les deux actions ont échoué.

  Solution : Voir *Impossible de supprimer le fichier à la page 6-91*.

- **Impossible de nettoyer ou renommer le fichier**

  Nettoyer est la première action. Renommer est la seconde action et les deux actions ont échoué.

  Solution : Voir *Impossible de mettre le fichier en quarantaine/Impossible de renommer le fichier à la page 6-90*.

- **Impossible de mettre le fichier en quarantaine/Impossible de renommer le fichier**

Explication 1

Le fichier infecté est peut-être verrouillé par une autre application, est en cours d'exécution ou se trouve sur un CD. OfficeScan mettra en quarantaine/renommera le fichier une fois que l'application aura terminé de traiter le fichier ou après son exécution.

Solution

Concernant les fichiers infectés sur un CD, Trend Micro déconseille l'utilisation de CD car le virus risque d'infecter les autres ordinateurs du réseau.

Explication 2

Le fichier infecté se trouve dans le dossier Temporary Internet Files de l'ordinateur client. Étant donné que l'ordinateur télécharge des fichiers pendant que vous naviguez, le navigateur Web a peut-être verrouillé le fichier infecté. Après que le navigateur Web a terminé le traitement du fichier, OfficeScan met en quarantaine/renomme le fichier.

Solution : Aucune

- **Impossible de supprimer le fichier**

  Explication 1

  Le fichier infecté est peut-être contenu dans un fichier compressé et le paramètre **Nettoyer/supprimer les fichiers infectés dans les fichiers compressés** dans **Ordinateurs en réseau** > **Paramètres clients généraux** est désactivé.

  Solution

  Activez l'option **Nettoyer/supprimer les fichiers infectés dans les fichiers compressés**. Lorsqu'il est activé, OfficeScan décompresse le fichier compressé, nettoie/supprime les fichiers infectés contenus dans le fichier compressé, puis le compresse à nouveau.

  Remarque

  Le choix de ce paramétrage est susceptible d'augmenter l'utilisation des ressources de l'ordinateur pendant le scan qui peut, de ce fait, durer plus longtemps.

Explication 2

Le fichier infecté est peut-être verrouillé par une autre application, est en cours d'exécution ou se trouve sur un CD. OfficeScan renommera le fichier une fois que l'application aura terminé de traiter le fichier ou après son exécution.

Solution

Concernant les fichiers infectés sur un CD, Trend Micro déconseille l'utilisation de CD car le virus risque d'infecter les autres ordinateurs du réseau.

Explication 3

Le fichier infecté se trouve dans le dossier Temporary Internet Files de l'ordinateur client OfficeScan. Étant donné que l'ordinateur télécharge des fichiers pendant que vous naviguez, le navigateur Web a peut-être verrouillé le fichier infecté. Après que le navigateur web a terminé le traitement du fichier, OfficeScan procède à sa suppression.

Solution : Aucune

- **Impossible d'envoyer le fichier à mettre en quarantaine dans le dossier de quarantaine spécifié**

  Bien qu'OfficeScan ait correctement mis en quarantaine un fichier dans le dossier `\Suspect` de l'ordinateur client OfficeScan, le fichier ne peut pas être envoyé vers le répertoire de quarantaine indiqué.

  Solution

  Déterminez quel type de scan (scan manuel, scan en temps réel, scan programmé ou scan immédiat) a détecté le virus/programme malveillant, puis examinez le contenu du répertoire de quarantaine spécifié dans l'onglet **Ordinateurs en réseau > Gestion des clients > Paramètres > {Type de scan} > onglet Action**.

  Si le répertoire de quarantaine se trouve sur l'ordinateur du serveur OfficeScan ou sur un autre ordinateur du serveur OfficeScan :

  1. Vérifiez que le client peut se connecter au serveur.
  2. Si vous utilisez un répertoire de quarantaine au format URL :
     a. Assurez-vous que le nom de l'ordinateur que vous spécifiez après «http://» est correct.

b. Vérifiez la taille du fichier infecté. Si elle excède la taille de fichier maximale spécifiée dans **Administration** > **Gestionnaire de quarantaine**, ajustez le paramètre pour l'adapter au fichier. Vous pouvez également effectuer d'autres actions, comme la suppression du fichier.

c. Vérifiez la taille du dossier de quarantaine et déterminez si celui-ci dépasse la capacité spécifiée dans **Administration** > **Gestionnaire de quarantaine**. Ajustez la capacité du dossier ou supprimez manuellement les fichiers du répertoire de quarantaine.

3. Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe «Tous» et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe. Vérifiez également que le répertoire de quarantaine existe et que le chemin UNC est correct.

Si le répertoire de quarantaine se trouve sur un autre ordinateur du réseau (vous ne pouvez utiliser qu'un chemin UNC pour ce scénario) :

1. Vérifiez que le client OfficeScan peut se connecter à l'ordinateur.
2. Vérifiez que le répertoire de quarantaine est partagé avec le groupe «Tous» et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe.
3. Vérifiez que le répertoire de quarantaine existe.
4. Vérifiez que le chemin UNC est correct.

Si le répertoire de quarantaine se trouve sur un répertoire différent de l'ordinateur client OfficeScan (vous ne pouvez utiliser qu'un chemin absolu pour ce scénario), vérifiez que le répertoire de quarantaine existe.

- **Impossible de nettoyer le fichier**

  Explication 1

  Le fichier infecté est peut-être contenu dans un fichier compressé et le paramètre Nettoyer/supprimer les fichiers infectés dans les fichiers compressés dans **Ordinateurs en réseau** > **Paramètres clients généraux** est désactivé.

  Solution

  Activez l'option **Nettoyer/supprimer les fichiers infectés dans les fichiers compressés**. Lorsqu'il est activé, OfficeScan décompresse le fichier compressé,

nettoie/supprime les fichiers infectés contenus dans le fichier compressé, puis le compresse à nouveau.

Remarque

Le choix de ce paramétrage est susceptible d'augmenter l'utilisation des ressources de l'ordinateur pendant le scan qui peut, de ce fait, durer plus longtemps.

Explication 2

Le fichier infecté se trouve dans le dossier Temporary Internet Files de l'ordinateur client OfficeScan. Étant donné que l'ordinateur télécharge des fichiers pendant que vous naviguez, le navigateur Web a peut-être verrouillé le fichier infecté. Après que le navigateur Web a terminé le traitement du fichier, OfficeScan procède à son nettoyage.

Solution : Aucune

Explication 3

Il se peut que le fichier ne puisse pas être nettoyé. Pour plus de détails et connaître les solutions, reportez-vous à *Fichier non nettoyable à la page C-17*.

Affichage des journaux de spywares/graywares

Le client OfficeScan génère des journaux lorsqu'il détecte des spywares et graywares, et les envoie au serveur.

Tâche

1. Accédez à l'un des emplacements suivants :
   - **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité**
   - **Ordinateurs en réseau** > **Gestion des clients**
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

3. Cliquez sur **Journaux** > **Journaux de spywares/graywares** ou **Afficher journaux** > **Journaux de spywares/graywares**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date et heure de la détection du spyware/grayware
   - Ordinateur affecté
   - Nom du spyware/grayware
   - Type de scan qui a détecté le spyware/grayware
   - Détails sur les résultats de scan anti-spywares/graywares (si l'action de scan a réussi ou non). Voir *Résultats de scan anti-spywares/graywares à la page 6-95* pour obtenir des informations détaillées.
   - adresse IP
   - Adresse MAC
   - Détails des journaux (Cliquez sur **Afficher** pour consulter les détails.)
6. Ajoutez les spywares/graywares que vous considérez inoffensifs à la Liste des spywares/graywares approuvés.
7. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

   Le fichier CSV contient les informations suivantes :
   - Toutes les informations dans les journaux
   - Nom d'utilisateur connecté à l'ordinateur au moment de la détection

---

Résultats de scan anti-spywares/graywares

Les résultats de scan suivants s'affichent dans les journaux de spywares/graywares :

- **Réussite. Aucune autre action requise**

Il s'agit du résultat de premier niveau si le scan est une réussite. Le résultat de deuxième niveau peut être l'un des suivants :

- **Nettoyés** : OfficeScan a mis fin aux processus ou supprimé les registres, fichiers, cookies et raccourcis.
- **Accès refusé** : OfficeScan a refusé l'accès (copie, ouverture) aux composants de spyware/grayware détectés.

- **Action supplémentaire requise**

  Il s'agit du résultat de premier niveau si le scan est un échec. Les résultats du deuxième niveau contiennent au moins l'un des messages suivants :

  - **Ignoré** : OfficeScan n'a entrepris aucune action mais a consigné la détection de spyware/grayware pour évaluation.

    Solution : ajoutez les spywares/graywares que vous considérez sans danger à la liste des spywares/graywares approuvés.

  - **Spywares/graywares dangereux à nettoyer** : ce message s'affiche si le moteur de scan anti-spywares tente de nettoyer un dossier unique et si les critères suivants sont remplis :

    - Les éléments à nettoyer dépassent 250 Mo.
    - Le système d'exploitation utilise les fichiers dans le dossier. Le dossier est également nécessaire pour le bon fonctionnement du système.
    - Le dossier est un répertoire racine (tel que `C:` ou `F:`)

    Solution : Contactez le service d'assistance pour obtenir de l'aide.

  - **Scan anti-spywares/graywares arrêté manuellement. Veuillez effectuer un scan complet** : un utilisateur a interrompu un scan avant qu'il soit achevé.

    Solution : exécutez un scan manuel et attendez que le scan soit achevé.

  - **Spyware/grayware nettoyé, redémarrage requis. Redémarrez l'ordinateur** : OfficeScan a nettoyé les composants de spyware/grayware, mais un redémarrage de l'ordinateur est requis pour terminer la tâche.

    Solution : redémarrez l'ordinateur immédiatement.

- **Impossible de nettoyer les spywares/graywares** : Un spyware/Grayware a été détecté sur un CD-ROM ou sur un lecteur de réseau. OfficeScan ne peut pas nettoyer les spywares/graywares détectés à ces emplacements.

  Solution : Supprimez manuellement le fichier infecté.

- **Résultat de scan anti-spywares/graywares inconnu. Contactez l'assistance technique de Trend Micro** : Une nouvelle version du moteur de scan anti-spyware fournit un nouveau résultat de scan que la configuration d'OfficeScan ne permet pas de traiter.

  Solution : contactez votre service d'assistance pour obtenir de l'aide afin de déterminer le nouveau résultat de scan.

Affichage des journaux de restauration de spywares/graywares

Après avoir nettoyé les spywares/graywares, les clients OfficeScan sauvegardent les données des spywares/graywares. Demandez aux clients en ligne de restaurer les données sauvegardées si vous considérez que les données sont inoffensives. Les informations relatives aux données de sauvegarde des spywares/graywares restaurées, à l'ordinateur concerné, et au résultat de la restauration sont disponibles dans les journaux.

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Restauration des spywares/graywares**.
2. Consultez la colonne **Résultat** pour vérifiez si OfficeScan a réussi la restauration des données de spywares/graywares.
3. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Journaux de scan

Lorsque le scan manuel, le scan programmé ou le scan immédiat s'exécute, le client OfficeScan créé un journal de scan contenant des informations sur le scan. Vous pouvez

consulter le journal de scan en accédant à la console du client OfficeScan. Les clients n'envoient pas le journal de scan au serveur.

Les journaux de scan présentent les informations suivantes :

- Date et heure à laquelle OfficeScan a commencé le scan
- Date et heure à laquelle OfficeScan a arrêté le scan
- État du scan
    - **Terminé** : Le scan s'est terminé sans problème.
    - **Arrêté** : L'utilisateur a interrompu le scan avant qu'il ne soit achevé.
    - **Arrêté de manière inattendue** : Le scan a été interrompu par l'utilisateur, le système, ou par un événement inattendu. Par exemple, il se peut que le service de scan en temps réel OfficeScan se soit terminé de façon inattendue ou que l'utilisateur ait effectué le redémarrage forcé du client.
- Type de scan
- Nombre d'objets scannés
- Nombre de fichiers infectés
- Nombre d'actions ayant échoué
- Nombre d'actions ayant réussi
- Version du fichier de signatures de virus
- Version de Smart Scan Agent Pattern
- Version du fichier de signatures de spywares

Épidémies de risques liés à la sécurité

Une épidémie de risques se déclare lorsque les détections de virus/programmes malveillants, spywares/graywares et sessions de partage de dossiers dépassent le seuil défini sur une certaine période. Il existe plusieurs manières de répondre et de contenir des épidémies sur le réseau, notamment:

- Activation d'OfficeScan pour surveiller le réseau à la recherche de toute activité suspecte
- Blocage des dossiers et des ports importants des ordinateurs clients
- Envoi aux clients des messages d'alerte d'épidémie
- Nettoyage des ordinateurs infectés

Critères et notifications d'épidémies de risques liés à la sécurité

Configurez OfficeScan afin que vous et les autres administrateurs OfficeScan receviez une notification lorsque l'un des événements suivants survient :

- Épidémie de virus/programmes malveillants
- Épidémie de spywares/graywares
- Épidémies de violation du pare-feu
- Épidémie de sessions de partage de dossiers

Définissez une épidémie selon le nombre de détections et la période de détection. Une épidémie se déclenche lorsque le nombre de détections dépasse le seuil défini au cours de la période de détection.

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, d'une épidémie. Vous pouvez modifier les notifications et configurer des paramètres de notification supplémentaires qui répondent à vos exigences.

Remarque

OfficeScan peut vous envoyer des notifications d'épidémies de risques liés à la sécurité par e-mail, pageur, déroutement SNMP et par les journaux d'événements de Windows NT. Pour les épidémies de sessions de partage de dossiers, OfficeScan envoie des notifications par e-mail. Configurez les paramètres lorsqu'OfficeScan envoie des notifications par le biais de ces chaînes. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 12-32*.

Configuration des critères et notifications d'épidémies de risques liés à la sécurité

Tâche

1. Accédez à **Notifications** > **Notifications administrateur** > **Notifications d'épidémies**.

2. Dans l'onglet **Critères** :

   a. Accédez aux sections **Virus/Programmes malveillants** et **Spyware/ Grayware** :

   b. Spécifiez le nombre de sources uniques de détections.

   c. Déterminez le nombre de détections et la période de détection pour chaque risque de sécurité.

Conseil

Trend Micro recommande d'accepter les valeurs par défaut dans cet écran.

OfficeScan envoie un message de notification lorsque le nombre de détections est dépassé. Par exemple, sous la section **Virus/Programmes malveillants**, si vous spécifiez 10 sources uniques, 100 détections et une durée de 5 heures, OfficeScan envoie une notification lorsque 10 clients différents reportent un nombre total de 101 risques de sécurité sur une période de 5 heures. Si toutes les détections effectuées au cours de la période de 5 heures concernent un seul point final, OfficeScan n'envoie pas de notification.

3. Dans l'onglet **Critères** :

   a. Accédez à la section **Sessions de partage de dossiers**.

   b. Sélectionnez **Contrôler les sessions de partage de dossiers sur votre réseau**.

   c. Sous **Sessions de partage de dossiers enregistrées**, cliquez sur le lien numéroté pour afficher les ordinateurs hébergeant des dossiers partagés et les ordinateurs accédant aux dossiers partagés.

d. Indiquez le nombre de sessions de partage de dossiers ainsi que la période de détection.

OfficeScan envoie un message de notification lorsque le nombre de sessions de partage de dossiers est dépassé.

4. Dans l'onglet **Courrier électronique** :

a. Accédez aux sections **Épidémies de virus/programmes malveillants**, **Épidémies de spywares/graywares** et **Épidémies de sessions de partage de dossiers**.

b. Sélectionnez **Activer la notification par courrier électronique**.

c. Indiquez les destinataires de l'e-mail.

d. Acceptez ou modifiez l'objet et le message par défaut de l'e-mail. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 6-20. Variables de jetons pour les notifications d'épidémies de risques liés à la sécurité

VARIABLE	DESCRIPTION
Épidémies de virus/programmes malveillants	
%CV	Nombre total de virus/programmes malveillants détectés
%CC	Nombre total d'ordinateurs infectés par des virus/programmes malveillants
Épidémies de spywares/graywares	
%CV	Nombre total de spywares/graywares détectés
%CC	Nombre total d'ordinateurs infectés par des spywares/graywares
Épidémies de sessions de partage de dossiers	
%S	Nombre de sessions de partage de dossiers
%T	Période d'accumulation des sessions de partage de dossiers
%M	Période, exprimée en minutes

e. Sélectionnez des informations supplémentaires sur les virus/programmes malveillants et les spywares/graywares à inclure dans l'e-mail. Vous pouvez inclure le nom du client/domaine, le nom du risque de sécurité, la date et l'heure de la détection, le chemin d'accès du fichier infecté et le résultat du scan.

f. Acceptez ou modifiez les messages de notification par défaut.

5. Dans l'onglet **Pageur** :

   a. Accédez aux sections **Épidémies de virus/programmes malveillants** et **Épidémies de spywares/graywares**.

   b. Sélectionnez **Activer la notification par pageur.**

   c. Saisissez le message.

6. Dans l'onglet **Déroutement SNMP**.

   a. Accédez aux sections **Épidémies de virus/programmes malveillants** et **Épidémies de spywares/graywares**.

   b. Sélectionnez **Activer la notification par déroutement SNMP**.

   c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 6-20 à la page 6-101* pour obtenir des informations détaillées.

7. Dans l'onglet **Journal des événements NT** :

   a. Accédez aux sections **Épidémies de virus/programmes malveillants** et **Épidémies de spywares/graywares**.

   b. Sélectionnez **Activer la notification via le journal d'événements NT**.

   c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 6-20 à la page 6-101* pour obtenir des informations détaillées.

8. Cliquez sur **Enregistrer**.

Configuration de la prévention des épidémies de risques liés à la sécurité

Lorsqu'une épidémie se produit, appliquez les mesures de prévention des épidémies pour répondre à l'épidémie et la contenir. Configurez soigneusement les paramètres de prévention car une mauvaise configuration peut entraîner des problèmes de réseau imprévus.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention des épidémies**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur l'une des stratégies suivantes de prévention des épidémies, puis configurez les paramètres qui s'y appliquent :
   - *Limitation/interdiction de l'accès aux dossiers partagés à la page 6-104*
   - *Blocage des ports vulnérables à la page 6-105*
   - *Interdiction de l'accès en écriture aux fichiers et dossiers à la page 6-107*
5. Sélectionnez les stratégies à appliquer.
6. Sélectionnez le nombre d'heures pendant lesquelles la prévention des épidémies sera active. La valeur par défaut est fixée à 48 heures. Vous pouvez restaurer manuellement les paramètres du réseau avant l'expiration de la période de prévention des épidémies.

   AVERTISSEMENT!

   N'autorisez pas l'activation permanente de la prévention des épidémies. Pour bloquer ou refuser en permanence l'accès à certains fichiers, dossiers ou ports, modifiez directement les paramètres de l'ordinateur et du réseau au lieu d'utiliser OfficeScan.

7. Acceptez ou modifiez les messages de notification de client par défaut.

Remarque

Pour configurer OfficeScan pour qu'il vous envoie une notification en cas d'épidémie, accédez à **Notifications** > **Notifications administrateur** > **Notifications d'épidémies**.

8. Cliquez sur **Démarrer la notification d'épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

9. De retour dans l'arborescence client, observez la colonne **Prévention des épidémies**.

   Une coche apparaît sur les ordinateurs qui appliquent des mesures de prévention des épidémies.

OfficeScan consigne les événements suivants dans les journaux d'événements du système :

- Événements liés aux serveurs (qui lancent le processus de prévention des épidémies et envoient aux clients des notifications leur demandant d'activer cette prévention)
- Événements liés au client OfficeScan (qui activent la prévention)

Stratégies de prévention des épidémies

Lorsqu'une épidémie se produit, appliquez l'une des stratégies suivantes :

- *Limitation/interdiction de l'accès aux dossiers partagés à la page 6-104*
- *Blocage des ports vulnérables à la page 6-105*
- *Interdiction de l'accès en écriture aux fichiers et dossiers à la page 6-107*

Limitation/interdiction de l'accès aux dossiers partagés

Pendant les épidémies, vous pouvez limiter ou interdire l'accès aux dossiers partagés sur le réseau pour empêcher la propagation des risques de sécurité à travers les dossiers partagés.

Lorsque cette stratégie entre en vigueur, les utilisateurs peuvent continuer de partager des dossiers mais elle ne s'applique pas aux dossiers qui viennent d'être partagés. Vous devez donc informer les utilisateurs pour qu'ils ne partagent pas les dossiers au cours d'une épidémie ou déployer de nouveau la stratégie pour l'appliquer aux dossiers qui viennent d'être partagés.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention des épidémies**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Limitation/interdiction de l'accès aux dossiers partagés**.
5. Sélectionnez l'une des options suivantes :
   - **Autoriser l'accès en lecture seule**: limite l'accès aux dossiers partagés
   - **Refuser tout accès**

   Remarque

   le paramètre d'accès en lecture seule ne s'applique pas aux dossiers partagés déjà configurés pour interdire tout accès.
6. Cliquez sur **Enregistrer**.

   L'écran Paramètres de prévention des épidémies s'affiche de nouveau.
7. Cliquez sur **Démarrer la notification d'épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Blocage des ports vulnérables

Pendant les épidémies, bloquez les ports vulnérables que les virus/programmes malveillants pourraient exploiter pour accéder aux ordinateurs clients OfficeScan.

AVERTISSEMENT!

Configurez alors les paramètres de prévention des épidémies avec soin. Le blocage des ports utilisés rendra indisponibles les services réseau qui dépendent de ces ports. Par exemple, si vous bloquez le port sécurisé, OfficeScan ne peut plus communiquer avec le client pendant l'épidémie.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention des épidémies**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Blocage des ports**.
5. Choisissez de bloquer ou non le port sécurisé.
6. Sélectionnez les ports à bloquer dans la colonne **Ports bloqués**.
   a. Si aucun port ne figure dans le tableau, cliquez sur **Ajouter**. Dans l'écran qui s'affiche, sélectionnez les ports à bloquer puis cliquez sur **Enregistrer**.
      - **Tous les ports (y compris ICMP)** : bloque tous les ports sauf le port sécurisé. Pour bloquer également le port sécurisé, cochez la case Bloquer le port sécurisé dans l'écran précédent.
      - **Ports fréquemment utilisés** : sélectionnez au moins un numéro de port pour permettre à OfficeScan d'enregistrer les paramètres de blocage de ports.
      - **Ports des chevaux de Troie** : bloque les ports habituellement utilisés par les programmes de type Cheval de Troie. Voir *Port des chevaux de Troie à la page C-14* pour obtenir des informations détaillées.
      - **Un numéro de port ou une plage de ports** : vous pouvez indiquer de façon facultative la direction du trafic à bloquer et certains commentaires, comme la raison pour laquelle vous bloquez les ports spécifiés.

- **Protocole de ping (Rejeter ICMP)** : cliquez ici pour bloquer uniquement les paquets ICMP, tels que les requêtes ping.

b. Pour modifier les paramètres du ou des ports bloqués, cliquez sur le numéro du port.

c. Dans l'écran qui s'affiche, modifiez les paramètres puis cliquez sur **Enregistrer**.

d. Pour supprimer un port de la liste, sélectionnez la case à cocher en regard du numéro de port puis cliquez sur **Supprimer**.

7. Cliquez sur **Enregistrer**.

L'écran Paramètres de prévention des épidémies s'affiche de nouveau.

8. Cliquez sur **Démarrer la notification d'épidémies**.

Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Interdiction de l'accès en écriture aux fichiers et dossiers

Les virus/programmes malveillants peuvent modifier ou supprimer les fichiers et les dossiers stockés sur les ordinateurs infectés. En cas d'épidémie, configurez OfficeScan de telle sorte que les virus/programmes malveillants ne puissent pas modifier ni supprimer les fichiers et les dossiers des postes clients OfficeScan.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention des épidémies**.

2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

3. Cliquez sur **Démarrer la prévention des épidémies**.

4. Cliquez sur **Interdire l'accès en écriture aux fichiers et dossiers**.

5. Entrez le chemin du répertoire. Lorsque vous aurez saisi le chemin d'accès au répertoire que vous souhaitez protéger, cliquez sur **Ajouter**.

Remarque

Saisissez le chemin d'accès absolu au répertoire, et non le chemin d'accès virtuel.

6. Spécifiez les fichiers à protéger dans les répertoires protégés. Sélectionnez tous les fichiers ou uniquement les fichiers avec une extension déterminée. Pour les extensions de fichiers, spécifiez une extension qui ne figure pas dans la liste proposée en la saisissant dans la zone de texte, puis en cliquant sur **Ajouter**.
7. Pour protéger des fichiers spécifiques, sous **Fichiers à protéger**, entrez le nom de fichier complet et cliquez sur **Ajouter**.
8. Cliquez sur **Enregistrer**.

   L'écran Paramètres de prévention des épidémies s'affiche de nouveau.
9. Cliquez sur **Démarrer la notification d'épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Désactivation de la prévention des épidémies

Si vous êtes absolument certain que l'épidémie détectée a été contenue et qu'OfficeScan a déjà nettoyé ou mis en quarantaine tous les fichiers infectés, rétablissez les valeurs normales de vos paramètres réseau en désactivant la fonction de prévention des épidémies.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention des épidémies**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Rétablir les paramètres**.
4. Pour informer les utilisateurs que l'épidémie est terminée, sélectionnez **Avertir les utilisateurs clients une fois les paramètres d'origine restaurés.**.
5. Acceptez ou modifiez les messages de notification de client par défaut.

6. Cliquez sur **Rétablir les paramètres**.

Remarque

Si vous ne restaurez pas les paramètres réseau manuellement, OfficeScan les restaure automatiquement après expiration du nombre d'heures spécifié dans **Restaurer automatiquement les paramètres initiaux du réseau après __ heures** dans l'écran **Paramètres de prévention des épidémies**. La valeur par défaut est fixée à 48 heures.

OfficeScan consigne les événements suivants dans les journaux d'événements du système :

- Événements liés aux serveurs (qui lancent le processus de prévention des épidémies et envoient aux clients OfficeScan des notifications leur demandant d'activer cette prévention)
- Événements liés au client OfficeScan (qui activent la prévention)

7. Après avoir désactivé la prévention des épidémies, recherchez les risques liés à la sécurité sur les ordinateurs en réseau pour vous assurer que l'épidémie a été contenue.

Chapitre 7

Utilisation de la surveillance des comportements

Ce chapitre explique comment protéger les ordinateurs des risques de sécurité en utilisant la fonctionnalité de surveillance des comportements.

Sujets abordés dans ce chapitre :

- *Surveillance des comportements à la page 7-2*
- *Privilèges de surveillance des comportements à la page 7-10*
- *Notifications de surveillance des comportements pour les utilisateurs du client OfficeScan à la page 7-11*
- *Journaux de surveillance des comportements à la page 7-13*

Surveillance des comportements

La surveillance des comportements surveille continuellement les points finaux, guettant les modifications inhabituelles du système d'exploitation ou des logiciels installés. La surveillance des comportements protège les points finaux via le **blocage du comportement des programmes malveillants** et la **surveillance des événements**. Une **liste d'exceptions** configurée par l'utilisateur et **Certified Safe Software Service** viennent compléter ces deux fonctionnalités.

Important

La surveillance des comportements ne prend pas en charge les plates-formes 64 bits Windows XP ou Windows 2003.

La surveillance des comportements prend en charge les plates-formes 64 bits Windows Vista SP1 ou version ultérieure.

Par défaut, la surveillance des comportements est désactivée pour toutes les versions de Windows Server 2003 et Windows Server 2008. Avant d'activer la surveillance des comportements sur ces plates-formes serveur, consultez les instructions et pratiques recommandées décrites dans *Services du client OfficeScan à la page 13-7*.

Blocage du comportement des programmes malveillants

Le blocage du comportement des programmes malveillants fournit un niveau nécessaire de protection supplémentaire contre les menaces pour les programmes qui affichent un comportement malveillant. Il observe les événements du système sur une période de temps. Pendant que les programmes exécutent différentes combinaisons ou séquences d'actions, le blocage du comportement des programmes malveillants détecte les comportements malveillants connus et bloque les programmes associés. Utilisez cette fonctionnalité pour vous assurer un niveau de protection plus élevé contre les menaces nouvelles, inconnues et émergentes.

Lorsqu'un programme est bloqué et que les notifications sont activées, OfficeScan affiche une notification sur l'ordinateur du client OfficeScan. Pour plus de détails sur les notifications, voir *Notifications de surveillance des comportements pour les utilisateurs du client OfficeScan à la page 7-11*.

Surveillance des événements

La surveillance des événements fournit une approche plus générique de la protection contre les logiciels non autorisés et les attaques de programmes malveillants. Elle surveille les zones du système pour certains événements, permettant aux administrateurs de gérer les programmes qui déclenchent ces événements. Utilisez la surveillance des événements si vous avez des exigences de protection du système spécifiques différentes de la protection fournie par le blocage du comportement des programmes malveillants.

Le tableau suivant répertorie les événements du système surveillés.

TABLEAU 7-1. ÉVÉNEMENTS DU SYSTÈME SURVEILLÉS

ÉVÉNEMENTS	DESCRIPTION
Fichier système dupliqué	Bon nombre de programmes malveillants créent des copies d'eux-mêmes ou d'autres programmes malveillants en se servant de noms de fichiers utilisés par les fichiers système Windows. Ceci a généralement pour but d'écraser ou de remplacer ces fichiers système, d'éviter la détection ou de décourager les utilisateurs de supprimer les programmes malveillants.
Modification du fichier Hosts	Le fichier Hosts établit la correspondance entre les noms de domaine et les adresses IP. De nombreux programmes malveillants modifient le fichier Hosts de telle sorte que le navigateur Web soit redirigé vers des sites Web infectés, inexistants ou contrefaits.
Comportement suspect	Le comportement suspect peut être une action spécifique ou une série d'actions inhabituelles de la part de programmes légitimes. Les programmes présentant un comportement suspect doivent être employés avec la plus grande prudence.
Nouveau plug-in Internet Explorer	Les programmes malveillants de type spywares/graywares installent souvent des plug-ins Internet Explorer indésirables, tels que des barres d'outils ou des outils d'aide à la navigation (BHO - Browser Helper Objects).
Modification des paramètres d'Internet Explorer	De nombreux virus/programmes malveillants modifient les paramètres d'Internet Explorer, notamment la page d'accueil, les sites Web de confiance, les paramètres de serveur proxy et les extensions de menu.

ÉVÉNEMENTS	DESCRIPTION
Modification des stratégies de sécurité	La modification des stratégies de sécurité de Windows peut permettre à des applications indésirables de s'exécuter puis de changer les paramètres du système.
Injection de bibliothèques de programmes	De nombreux programmes malveillants configurent Windows de telle sorte que toutes les applications chargent automatiquement une bibliothèque de programmes (DLL). Ceci permet aux routines malveillantes contenues dans cette DLL de s'exécuter chaque fois qu'une de ces applications est lancée.
Modification du shell	De nombreux programmes malveillants modifient les paramètres du shell Windows de manière à s'associer eux-mêmes à certains types de fichiers. Cette routine permet à des programmes malveillants de se lancer automatiquement dès qu'un utilisateur ouvre les fichiers associés dans l'Explorateur Windows. La modification des paramètres du shell Windows peut aussi permettre à des programmes malveillants de suivre les programmes utilisés et de s'exécuter conjointement avec les applications légitimes.
Nouveau service	Les services Windows sont des processus dotés de fonctions spéciales qui, généralement, s'exécutent continuellement en arrière-plan et bénéficient d'un accès d'administration complet. Certains programmes malveillants s'installent eux-mêmes en tant que services afin de rester dissimulés.
Modification du système de fichiers	Certains fichiers système de Windows déterminent le comportement du système et notamment les paramètres relatifs aux programmes de démarrage et aux économiseurs d'écran. De nombreux programmes malveillants modifient les fichiers système de manière à s'exécuter automatiquement au démarrage et contrôler le comportement du système.
Modification des stratégies de pare-feu	La stratégie de pare-feu Windows détermine quelles applications ont accès au réseau, quels ports sont ouverts à la communication et quelles adresses IP peuvent communiquer avec l'ordinateur. De nombreux programmes malveillants modifient la stratégie de manière à s'octroyer à eux-mêmes l'accès au réseau et à Internet.

ÉVÉNEMENTS	DESCRIPTION
Modification des processus système	De nombreux programmes malveillants agissent de différentes façons sur les processus Windows intégrés. Ces actions peuvent consister à interrompre ou à modifier les processus en cours d'exécution.
Nouveau programme de démarrage	De nombreux programmes malveillants configurent Windows de telle sorte que toutes les applications chargent automatiquement une bibliothèque de programmes (DLL). Ceci permet aux routines malveillantes contenues dans cette DLL de s'exécuter chaque fois qu'une de ces applications est lancée.

Lorsque la surveillance des événements détecte un événement du système surveillé, elle exécute l'action configurée pour l'événement.

Le tableau suivant répertorie les éventuelles mesures que les administrateurs peuvent prendre sur les événements du système surveillés.

TABLEAU 7-2. Actions sur les événements du système surveillés

ACTION	DESCRIPTION
Évaluer	OfficeScan autorise toujours les programmes associés à un événement, mais enregistre cette action dans les journaux pour évaluation. Il s'agit de l'action par défaut pour tous les événements du système surveillés. **Remarque** Cette option n'est pas prise en charge pour l'injection de bibliothèques de programmes sur les systèmes 64 bits.
Autoriser	OfficeScan autorise toujours les programmes associés à un événement.

ACTION	DESCRIPTION
Demander si nécessaire	OfficeScan invite les utilisateurs à autoriser ou refuser les programmes associés à un événement et ajoute les programmes à la liste d'exceptions Si l'utilisateur ne répond pas au cours d'une certaine période, OfficeScan autorise automatiquement l'exécution du programme. La valeur par défaut de la période est 30 secondes. Pour modifier la période, reportez-vous à *Modification de la période avant l'autorisation de l'exécution d'un programme à la page 7-8*. **Remarque** Cette option n'est pas prise en charge pour l'injection de bibliothèques de programmes sur les systèmes 64 bits.
Refuser	OfficeScan bloque toujours les programmes associés à un événement et enregistre cette action dans les journaux. Lorsqu'un programme est bloqué et que les notifications sont activées, OfficeScan affiche une notification sur l'ordinateur du client OfficeScan. Pour plus de détails sur les notifications, voir *Notifications de surveillance des comportements pour les utilisateurs du client OfficeScan à la page 7-11*.

Liste d'exceptions de la surveillance des comportements

La liste d'exceptions de la surveillance des comportements contient les programmes n'étant pas surveillés par la surveillance des comportements.

- **Programmes approuvés** : Les programmes de cette liste peuvent être exécutés. Un programme approuvé sera toutefois vérifié par d'autres fonctionnalités de OfficeScan (telles qu'un scan des fichiers) avant que son exécution ne soit définitivement autorisée.
- **Programmes bloqués** : Les programmes de cette liste ne peuvent jamais être démarrés. Pour configurer cette liste, la surveillance des événements doit être activée.

Configurez la liste d'exceptions depuis la console Web. Vous pouvez également donner aux utilisateurs le privilège de configurer leur propre liste d'exceptions depuis la console

du client OfficeScan. Pour obtenir des informations détaillées, voir *Privilèges de surveillance des comportements à la page 7-10*.

Configuration du blocage du comportement des programmes malveillants, de la surveillance des événements et de la liste Exception

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de surveillance des comportements**.
4. Sélectionnez **Activer le blocage du comportement des programmes malveillants**.
5. Configurez les paramètres de surveillance des comportements.
   a. Sélectionnez **Activer la surveillance des événements**.
   b. Choisissez les événements du système à surveiller et sélectionnez une action pour chacun de ces événements. Pour des informations relatives aux événements du système surveillés et aux actions, voir *Surveillance des événements à la page 7-3*.
6. Configurez la liste d'exceptions.
   a. Sous **Saisissez le chemin d'accès complet au programme**, entrez le chemin d'accès complet du programme à approuver ou à bloquer. Séparez les entrées multiples par des points virgules (;). La liste d'exceptions prend en charge les caractères génériques et les chemins UNC.
   b. Cliquez sur **Approuver les programmes ou Bloquer les programmes**.
   c. Pour supprimer de la liste un programme approuvé ou bloqué, cliquez sur l'icône corbeille ( ) à côté du programme.

Remarque

OfficeScan accepte au maximum 100 programmes approuvés et 100 programmes bloqués.

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Modification de la période avant l'autorisation de l'exécution d'un programme

Ce paramètre fonctionne uniquement si la surveillance des événements est activée et si l'action pour un événement du système surveillé est «Demander si nécessaire». Cette action demande à l'utilisateur d'autoriser ou de refuser les programmes associés à l'événement. Si l'utilisateur ne répond pas au cours d'une certaine période, OfficeScan autorise automatiquement l'exécution du programme. Pour obtenir des informations détaillées, voir *Surveillance des événements à la page 7-3*.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Accédez à la section **Paramètres de surveillance des comportements**.
3. Précisez la période dans **Autoriser automatiquement le programme si le client ne répond pas dans les __ secondes**.
4. Cliquez sur **Enregistrer**.

Certified Safe Software Service

Le service Certified Safe Software Service interroge les centres de données Trend Micro pour vérifier la sécurité d'un programme détecté par le blocage du comportement des programmes malveillants ou la surveillance des événements. Activez le service Certified Safe Software Service pour réduire la probabilité de détection de faux-positifs.

Remarque

Vérifiez que les clients OfficeScan disposent des paramètres proxy corrects (pour plus d'informations, voir *Paramètres proxy du client OfficeScan à la page 13-50*) avant d'activer Certified Safe Software Service. Des paramètres proxy incorrects, de même qu'une connexion Internet intermittente, peuvent entraîner des retards ou un échec de réception d'une réponse des centres de données Trend Micro, et faire que des programmes apparaissent comme sans réponse.

De plus, des clients OfficeScan possédant une adresse IPv6 pure ne peuvent interroger directement depuis les centres de données Trend Micro. Un serveur proxy double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients OfficeScan de se connecter aux centres de données Trend Micro.

Activation de Certified Safe Software Service

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Accédez à la section **Paramètres de surveillance des comportements**.
3. Sélectionnez l'option **Activer Certified Safe Software Service**.
4. Cliquez sur **Enregistrer**.

Privilèges de surveillance des comportements

Si les clients disposent des privilèges de surveillance des comportements, l'onglet Surveillance des comportements s'affiche sur la console du client OfficeScan. Les utilisateurs peuvent alors gérer leur propre liste d'exceptions.

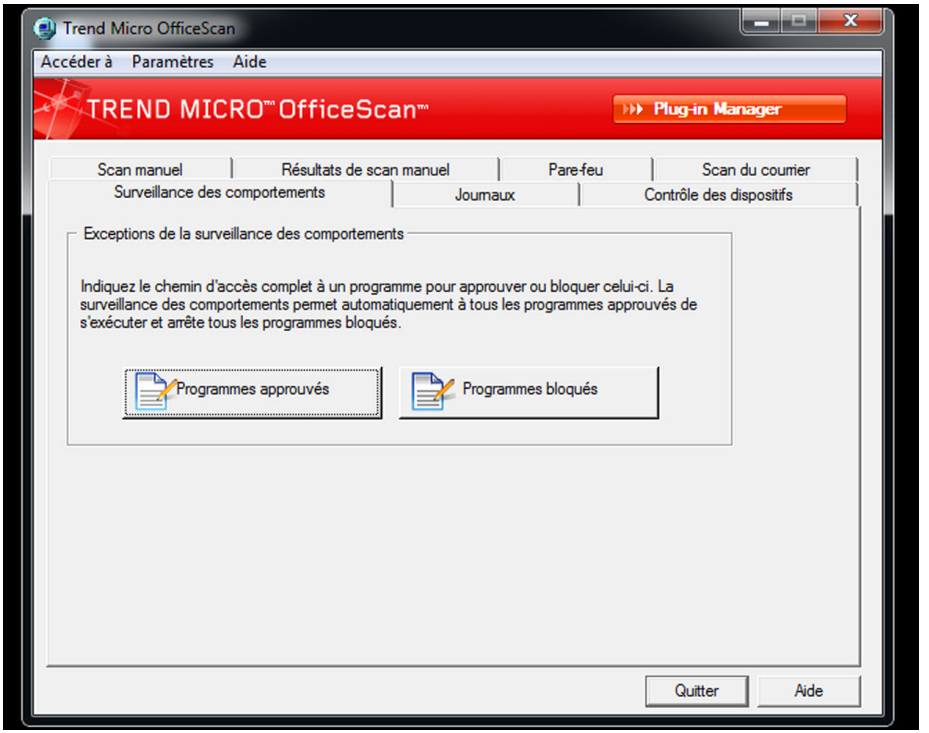


FIGURE 7-1. Onglet Surveillance des comportements sur la console du client OfficeScan

Autorisation de privilèges de surveillance des comportements

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de surveillance des comportements**.
5. Sélectionnez **Afficher l'onglet Surveillance des comportements sur la console du client**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Notifications de surveillance des comportements pour les utilisateurs du client OfficeScan

OfficeScan peut afficher un message de notification sur un ordinateur du client OfficeScan immédiatement après que la surveillance des comportements a bloqué un

programme. Activer l'envoi de messages de notification et modifier éventuellement le contenu du message.

Activation de l'envoi de messages de notification

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Paramètres de surveillance des comportements**.
5. Sélectionnez **Afficher une notification lorsqu'un programme est bloqué**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Modification du contenu du message de notification

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.

2. Cliquez sur l'onglet **Violations de la stratégie de surveillance des comportements**.
3. Saisissez le message par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de surveillance des comportements

Les clients OfficeScan consignent dans des journaux les accès à des programmes non autorisés et envoient ces journaux au serveur. Un client OfficeScan qui s'exécute en permanence regroupe les journaux et les envoie à un intervalle spécifié, qui est de 60 minutes par défaut.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de surveillance des comportements

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité** ou à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Journaux** > **Journaux de surveillance des comportements** ou **Afficher les journaux** > **Journaux de surveillance des comportements**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date/heure de détection du processus non autorisé

- Ordinateur sur lequel le processus non autorisé a été détecté
- Domaine de l'ordinateur
- Violation : règle de surveillance des événements avec laquelle le processus est en infraction
- Action exécutée lors de la détection de la violation
- Événement : type d'objet auquel le programme a accédé
- Niveau de risque que représente le programme non autorisé
- Programme, c'est-à-dire le programme non autorisé
- Opération : action exécutée par le programme non autorisé
- Cible, c'est-à-dire le processus qui a fait l'objet de l'accès

6. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Configuration de la programmation d'envoi de journaux de surveillance des comportements

Tâche

1. Accédez au <*dossier d'installation du serveur*>`\PCCSRV`.
2. Ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte comme le Bloc-notes.
3. Recherchez la chaîne « `SendBMLogPeriod` », puis vérifiez la valeur en regard de cette chaîne.

   La valeur par défaut est 3 600 secondes et la chaîne a l'aspect suivant : `SendBMLogPeriod=3600`.
4. Spécifiez la valeur en secondes.

Par exemple, pour faire passer la période d'envoi des journaux à 2 heures, indiquez 7200 comme valeur.

5. Enregistrez le fichier.
6. Accédez à **Ordinateurs en réseau** > **Paramètres clients généraux**.
7. Cliquez sur **Enregistrer** sans changer aucun paramètre.
8. Redémarrez l'ordinateur client.

Chapitre 8

Utilisation du contrôle des dispositifs

Ce chapitre explique comment protéger les ordinateurs des risques de sécurité en utilisant la fonctionnalité de contrôle des dispositifs.

Sujets abordés dans ce chapitre :

- *Contrôle des dispositifs à la page 8-2*
- *Modification des notifications du contrôle des dispositifs à la page 8-17*
- *Journaux de contrôle des dispositifs à la page 8-17*

Contrôle des dispositifs

Le Contrôle des dispositifs régule l'accès aux périphériques de stockage externes et ressources réseau connectés aux ordinateurs. Le Contrôle des dispositifs prévient la perte et les fuites de données et, conjointement avec le scan de fichiers, contribue à la protection contre les risques de sécurité.

Vous pouvez configurer les stratégies de contrôle des dispositifs pour les clients internes et externes. Les administrateurs OfficeScan configurent généralement une stratégie plus stricte pour les clients externes.

Les stratégies sont des paramètres détaillés dans l'arborescence des clients OfficeScan. Vous pouvez appliquer des stratégies spécifiques à des groupes de clients ou à des clients individuels. Vous pouvez également appliquer une stratégie unique à tous les clients.

Une fois que vous avez déployé les stratégies, les clients utilisent les critères d'emplacement définis dans l'écran Emplacement de l'ordinateur (voir *Emplacement de l'ordinateur à la page 13-2*) afin de déterminer leur emplacement et la stratégie à appliquer. Les clients changent de stratégie à chaque fois que l'emplacement change.

Important :

- Par défaut, le contrôle des dispositifs est désactivé sur toutes les versions de Windows Server 2003 et Windows Server 2008. Avant d'activer le contrôle des dispositifs sur ces plates-formes serveur, consultez les instructions et pratiques recommandées décrites dans *Services du client OfficeScan à la page 13-7*.
- Les types de périphériques pouvant être surveillés par OfficeScan dépendent de l'activation de la licence de protection des données. La protection des données fait l'objet d'une licence distincte et doit être activée avant d'être utilisée. Pour plus d'informations sur la licence de protection des données, voir *Licence de protection des données à la page 9-4*.

TABLEAU 8-1. Types de périphériques

	PROTECTION DES DONNÉES ACTIVÉE	PROTECTION DES DONNÉES DÉSACTIVÉE
Périphériques de stockage		

	PROTECTION DES DONNÉES ACTIVÉE	PROTECTION DES DONNÉES DÉSACTIVÉE
CD/DVD	Surveillé	Surveillé
Disquettes	Surveillé	Surveillé
Lecteurs de réseau	Surveillé	Surveillé
Périphériques de stockage USB	Surveillé	Surveillé
Périphériques qui ne sont pas destinés au stockage		
Ports COM et LPT	Surveillé	Non surveillé
Interface IEEE 1394	Surveillé	Non surveillé
Périphériques d'images	Surveillé	Non surveillé
Périphériques infrarouges	Surveillé	Non surveillé
Modems	Surveillé	Non surveillé
Carte PCMCIA	Surveillé	Non surveillé
Touche Impr. écran	Surveillé	Non surveillé

- Pour obtenir la liste des modèles de périphériques pris en charge, voir :

  http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Autorisations pour les périphériques de stockage

Les autorisations du contrôle des dispositifs pour les périphériques de stockage sont utilisées dans les cas suivants :

- Lorsque vous autorisez l'accès aux périphériques de stockage USB, CD/DVD, disquettes et lecteurs de réseau. Vous pouvez accorder un accès complet ou limiter le niveau d'accès à ces périphériques.
- Configurez la liste des périphériques de stockage USB approuvés. Le contrôle des dispositifs vous permet de bloquer l'accès à tous les périphériques de stockage USB, sauf ceux qui ont été ajoutés à la liste des périphériques approuvés. Vous

pouvez accorder un accès complet aux périphériques approuvés ou limiter le niveau d'accès.

Le tableau suivant répertorie les autorisations d'accès aux périphériques de stockage.

TABLEAU 8-2. Autorisations de contrôle des dispositifs pour les périphériques de stockage

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Accès complet	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer, Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier En d'autres termes, un fichier peut être enregistré, déplacé et copié sur le périphérique.
Modifier	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer Opérations interdites : Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier
Lire et exécuter	Opérations autorisées : Copier, Ouvrir, Exécuter Opérations interdites : Enregistrer, Déplacer, Supprimer	Opérations interdites : Enregistrer, Déplacer, Copier
Lire	Opérations autorisées : Copier, Ouvrir Opérations interdites : Enregistrer, Déplacer, Supprimer, Exécuter	Opérations interdites : Enregistrer, Déplacer, Copier
Répertorier le contenu des dispositifs uniquement	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient sont visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Bloquer (disponible après l'installation de la protection des données)	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient ne sont pas visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier

La fonction de scan de fichiers d'OfficeScan complète et, le cas échéant, annule les autorisations relatives aux périphériques. Si, par exemple, l'une d'entre elles autorise l'ouverture d'un fichier mais qu'OfficeScan détecte que celui-ci est infecté par un programme malveillant, une action de scan spécifique est exécutée sur le fichier pour éliminer ce programme. Si l'action de scan est Nettoyer, le fichier s'ouvre une fois le nettoyage effectué. Si, en revanche l'action de scan est Supprimer, le fichier est supprimé.

Conseil

Le contrôle des dispositifs pour la protection des données prend en charge toutes les plates-formes 64 bits. Pour assurer la surveillance de la prévention des modifications non autorisées sur les systèmes non pris en charge par OfficeScan (pour en savoir plus, voir *Compatibilité du contrôle des dispositifs avec une architecture 64 bits lors de la prévention des modifications non autorisées à la page 1-3*), définissez les autorisations pour les dispositifs sur **Bloquer** pour limiter l'accès à ces périphériques.

Autorisations avancées pour les périphériques de stockage

Les autorisations avancées sont appliquées lorsque vous accordez des autorisations limitées aux périphériques de stockage. L'autorisation peut être :

- Modifier
- Lire et exécuter
- Lire
- Répertorier le contenu des dispositifs uniquement

Vous pouvez continuer de limiter les autorisations tout en accordant des autorisations avancées à certains programmes des périphériques de stockage et de l'ordinateur local.

Pour définir des programmes, configurez les listes de programmes suivantes.

TABLEAU 8-3. Listes des programmes

LISTE DES PROGRAMMES	DESCRIPTION	ENTRÉES VALIDES
Programmes disposant d'un accès en lecture et écriture aux périphériques	Cette liste contient des programmes locaux ainsi que des programmes de périphériques de stockage ayant un droit de lecture et d'écriture sur les périphériques. Microsoft Word (`winword.exe`) est un exemple de programme local. Il est généralement situé sous `C:\Program Files\Microsoft Office\Office`. Si l'autorisation d'accès aux périphériques de stockage USB est « Répertorier le contenu des dispositifs uniquement » mais que « `C:\Program Files\Microsoft Office\Office\winword.exe` » est inclus dans cette liste : • un utilisateur aura accès en lecture et écriture à tous les fichiers du périphérique de stockage USB accessibles avec Microsoft Word. • un utilisateur peut enregistrer, déplacer ou copier un fichier Microsoft Word dans le périphérique de stockage USB.	Nom et chemin d'accès du programme Pour obtenir des informations détaillées, voir *Spécification du nom et du chemin d'accès d'un programme à la page 8-8*.

LISTE DES PROGRAMMES	DESCRIPTION	ENTRÉES VALIDES
Programmes présents sur les périphériques qui sont autorisés à s'exécuter	Cette liste contient des programmes se trouvant sur les périphériques de stockage et que les utilisateurs ou le système peuvent exécuter. Par exemple, si vous souhaitez autoriser les utilisateurs à installer un logiciel à partir d'un CD, ajoutez le nom et le chemin d'accès du programme d'installation, comme « `E:\Installer\Setup.exe` », à cette liste.	Chemin d'accès et nom du programme ou fournisseur de la signature numérique Pour plus d'informations, voir *Spécification du nom et du chemin d'accès d'un programme à la page 8-8* ou *Spécification d'un fournisseur Digital Signature à la page 8-8*.

Dans certains cas vous devrez ajouter un programme aux deux listes. Prenez par exemple la fonctionnalité de verrouillage de données d'un périphérique de stockage USB qui, si elle est activée, invite l'utilisateur à fournir un nom et un mot de passe avant de déverrouiller le périphérique. La fonctionnalité de verrouillage de données utilise le programme « `Password.exe` » sur le périphérique. Il doit être autorisé à s'exécuter afin que les utilisateurs puissent déverrouiller le périphérique. "`Password.exe` » doit également disposer de droit de lecture et d'écriture sur le périphérique afin que les utilisateurs puissent modifier leur nom d'utilisateur ou leur mot de passe.

Chaque liste de programmes de l'interface utilisateur peut contenir jusqu'à 100 programmes. Si vous souhaitez ajouter plus de programmes à une liste de programmes, vous devrez les ajouter dans le fichier `ofcscan.ini` qui peut accepter un maximum de 1 000 programmes. Pour plus d'informations sur l'ajout de programmes dans le fichier `ofcscan.ini`, voir *Ajout de programmes aux listes de contrôle des dispositifs à l'aide du fichier ofcscan.ini à la page 8-15*.

AVERTISSEMENT!

Les programmes ajoutés au fichier `ofcscan.ini` seront déployés sur le domaine racine et remplaceront les programmes des clients ou domaines individuels.

Spécification d'un fournisseur Digital Signature

Spécifiez un fournisseur de signature digitale si vous faites confiance aux programmes de ce fournisseur. Par exemple, entrez Microsoft Corporation ou Trend Micro, Inc. Vous pouvez obtenir le fournisseur de signature digitale en vérifiant les propriétés d'un programme (par exemple, en cliquant avec le bouton droit sur le programme et en sélectionnant **Propriétés**).

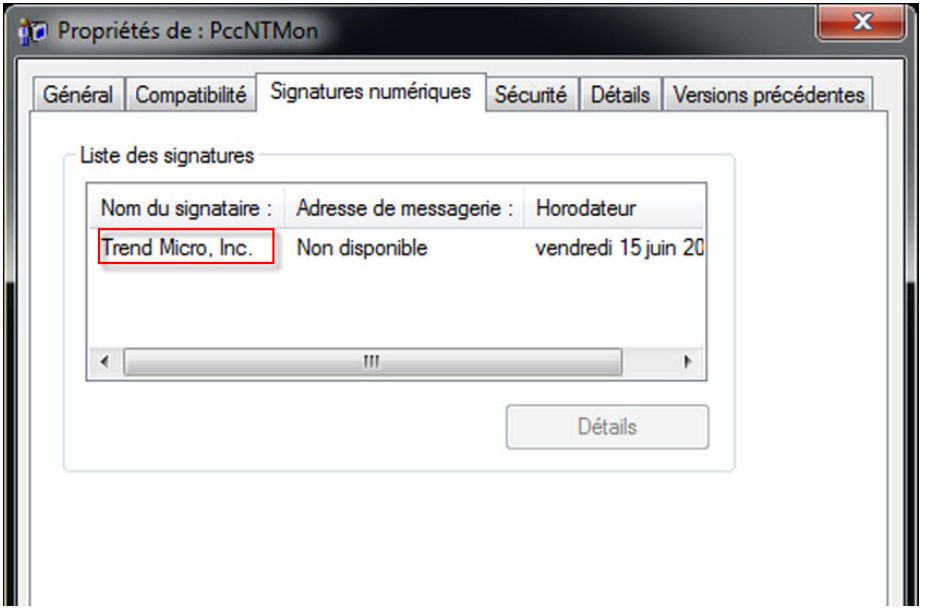


FIGURE 8-1. Fournisseur de Digital Signature pour le programme client OfficeScan (`PccNTMon.exe`)

Spécification du nom et du chemin d'accès d'un programme

Le nome et le chemin d'accès d'un programme doivent compter 259 caractères au maximum et ne peuvent contenir que des caractères alphanumérique (A-Z, a-z, 0-9). Il est impossible de spécifier uniquement le nom du programme.

Vous pouvez utiliser des caractères génériques pour remplacer les lettres de lecteur et les noms de programmes. Utilisez un point d'interrogation (?) pour remplacer un seul

caractère, comme la lettre d'un lecteur. Utilisez un astérisque (*) pour remplacer plusieurs caractères, comme un nom de programme.

Remarque

Les caractères génériques ne peuvent pas être utilisés pour remplacer des noms de dossiers. Le nom exact du dossier doit être spécifié.

Les caractères génériques peuvent être utilisés dans les exemples suivants :

TABLEAU 8-4. UTILISATION CORRECTE DES CARACTÈRES GÉNÉRIQUES

EXEMPLE	DONNÉES CORRESPONDANTES
?:\Password.exe	Le fichier «Password.exe» situé dans n'importe quel lecteur
C:\Program Files\Microsoft *.exe	Tout fichier sous C:\Program Files qui possède une extension de fichier
C:\Program Files*.*	Tout fichier sous C:\Program Files qui possède une extension de fichier
C:\Program Files\a**?**c.exe	Tout fichier .exe sous C:\Program Files dont le nom est composé de 3 caractères, commençant par la lettre « a » et se terminant par la lettre « c »
C:*	Tout fichier se trouvant directement sous C:\drive, qu'il possède ou non une extension de fichier

Les caractères génériques ne peuvent pas être utilisés dans les exemples suivants :

TABLEAU 8-5. UTILISATION INCORRECTE DES CARACTÈRES GÉNÉRIQUES

EXEMPLE	CAUSE
??:\Buffalo\Password.exe	?? représente deux caractères alors qu'une lettre de lecteur n'est composée que d'un seul caractère alphabétique.
*:\Buffalo\Password.exe	* représente plusieurs caractères alors qu'une lettre de lecteur n'est composée que d'un seul caractère alphabétique.

EXEMPLE	CAUSE
C:*\Password.exe	Les caractères génériques ne peuvent pas être utilisés pour remplacer des noms de dossiers. Le nom exact du dossier doit être spécifié.
C:\?\Password.exe	

Autorisations pour les périphériques qui ne sont pas destinés au stockage

Vous pouvez autoriser ou bloquer l'accès à des périphériques qui ne sont pas destinés au stockage. Il n'y a pas d'autorisation détaillée ou avancée pour ces périphériques.

Gestion de l'accès aux périphériques externes (protection des données activée)

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de contrôle des dispositifs**.
4. Pour configurer une stratégie applicable aux clients externes, cliquez sur l'onglet **Clients externes** ; pour configurer une stratégie applicable aux clients internes, cliquez sur **Clients internes**.
5. Sélectionnez **Activer le contrôle des dispositifs**.
6. Appliquez les paramètres comme suit :
   - Si vous vous trouvez dans l'onglet **Clients externes**, vous pouvez appliquer les paramètres aux clients internes en sélectionnant **Appliquer tous les paramètres aux clients internes**.
   - Si vous êtes dans l'onglet **Clients internes**, vous pouvez appliquer les paramètres aux clients externes en sélectionnant **Appliquer tous les paramètres aux clients externes**.

7. Autorisez ou bloquez la fonction AutoRun (`autorun.inf`) sur les périphériques de stockage USB.

8. Configurez les paramètres pour les périphériques de stockage.

   a. Sélectionnez une autorisation pour chaque périphérique de stockage. Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques de stockage à la page 8-3*.

   b. Si l'autorisation pour les périphériques de stockage USB est **Bloquer**, configurez une liste de périphériques approuvés. Les utilisateurs peuvent accéder à ces périphériques et vous pouvez contrôler le niveau d'accès en utilisant les autorisations. Voir la section *Configuration d'une liste approuvée de périphériques USB à la page 8-13*.

9. Pour chaque périphérique non destiné au stockage, sélectionnez **Autoriser** ou **Bloquer**.

10. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Configuration des autorisations avancées

Bien que vous puissiez configurer des autorisation avancées et des notifications pour un périphérique de stockage spécifique dans l'interface utilisateur, les autorisations et les notifications sont en fait attribuées à tous les périphériques de stockage. Cela signifie que lorsque vous cliquez sur **Autorisations avancées et notifications** pour un CD ou un DVD, vous définissez des autorisations et des notifications pour tous les périphériques de stockage.

Remarque

Pour plus d'informations sur les autorisations avancées et la manière de définir correctement des programmes avec des autorisations avancées, voir *Autorisations avancées pour les périphériques de stockage à la page 8-5*.

Tâche

1. Cliquez sur **Autorisations avancées et notifications**.

   Un nouvel écran s'affiche.

2. Sous **Programmes ayant un droit de lecture et d'écriture sur des périphériques des stockage**, entrez le nom et le chemin d'accès d'un programme, puis cliquez sur **Ajouter**.

   Le fournisseur de la signature digitale n'est pas accepté.

3. Sous **Programmes présents sur les périphériques de stockage et autorisés à s'exécuter**, entrez le nom et le chemin d'accès du programme ou le fournisseur de la signature digitale, puis cliquez sur **Ajouter**.

4. Sélectionnez **Afficher un message de notification sur l'ordinateur client lorsqu'OfficeScan détecte un accès non autorisé à un périphérique**.

   - Un accès non autorisé à un périphérique fait référence à des opérations interdites. Par exemple, si l'autorisation pour le périphérique est «Lire», les utilisateurs ne pourront pas enregistrer, déplacer, supprimer ou exécuter un fichier sur le périphérique. Pour une liste d'opérations interdites sur le périphériques sur base des autorisations, voir *Autorisations pour les périphériques de stockage à la page 8-3*.

   - Vous pouvez modifier le message de notification. Pour plus d'informations, voir *Modification des notifications du contrôle des dispositifs à la page 8-17*.

5. Cliquez sur **Retour**.

Configuration d'une liste approuvée de périphériques USB

Tâche

1. Cliquez sur **Périphériques approuvés**.
2. Entrez le nom du fournisseur de périphérique.
3. Entrez le modèle et le numéro de série.

> **Conseil**
>
> À l'aide de l'outil Liste de dispositifs, interrogez les dispositifs reliés aux points finaux. L'outil indique, pour chaque périphérique, le nom du fournisseur, le modèle et le numéro de série. Pour obtenir des informations détaillées, voir *Outil Liste de dispositifs à la page 9-54*.

4. Sélectionnez l'autorisation pour le périphérique. Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques de stockage à la page 8-3*.
5. Pour ajouter plusieurs périphériques, cliquez sur l'icône **+**.
6. Cliquez sur **Retour**.

Gestion de l'accès aux périphériques externes (protection des données non activée)

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres de contrôle des dispositifs**.
4. Pour configurer une stratégie applicable aux clients externes, cliquez sur l'onglet **Clients externes** ; pour configurer une stratégie applicable aux clients internes, cliquez sur **Clients internes**.
5. Sélectionnez **Activer le contrôle des dispositifs**.

6. Appliquez les paramètres comme suit :

   - Si vous vous trouvez dans l'onglet **Clients externes**, vous pouvez appliquer les paramètres aux clients internes en sélectionnant **Appliquer tous les paramètres aux clients internes**.
   - Si vous êtes dans l'onglet **Clients internes**, vous pouvez appliquer les paramètres aux clients externes en sélectionnant **Appliquer tous les paramètres aux clients externes**.

7. Autorisez ou bloquez la fonction AutoRun (`autorun.inf`) sur les périphériques de stockage USB.

8. Sélectionnez une autorisation pour chaque périphérique de stockage. Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques de stockage à la page 8-3*.

9. Configurez des autorisations avancées et des notifications si l'autorisation pour un périphérique de stockage est l'une des suivantes : **Modifier**, **Lire et exécuter**, **Lire** ou **Répertorier le contenu des dispositifs uniquement**. Voir la section *Configuration des autorisations avancées à la page 8-11*.

10. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Ajout de programmes aux listes de contrôle des dispositifs à l'aide du fichier ofcscan.ini

Remarque

Pour plus d'informations sur les listes de programmes et la manière de définir correctement les programmes pouvant être ajoutés à la liste, voir *Autorisations avancées pour les périphériques de stockage à la page 8-5*.

Tâche

1. Sur l'ordinateur du serveur OfficeScan, accédez au <*Dossier d'installation du serveur*>`\PCCSRV`.
2. Ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte.
3. Pour ajouter des programmes disposant d'un accès en lecture et écriture sur les périphériques de stockage :
   a. Localisez les lignes suivantes :

      ```
      [DAC_APPROVED_LIST]

      Count=x
      ```

   b. Remplacez «x» par le nombre de programmes de la liste de programmes.
   c. Sous «Count=x», ajoutez des programmes en entrant :

      ```
      Élément<numéro>=<chemin d'accès et nom du programme ou
      fournisseur de la signature numérique>
      ```

      Par exemple :

      ```
      [DAC_APPROVED_LIST]

      Count=3

      Item0=C:\Program Files\program.exe

      Item1=?:\password.exe

      Élément 2 = Microsoft Corporation
      ```

4. Pour ajouter des programmes présents sur les périphériques de stockage et autorisés à s'exécuter :

   a. Localisez les lignes suivantes :

   ```
   [DAC_EXECUTABLE_LIST]

   Count=x
   ```

   b. Remplacez «x» par le nombre de programmes de la liste de programmes.

   c. Sous «Count=x», ajoutez des programmes en entrant :

   ```
   Élément<numéro>=<chemin d'accès et nom du programme ou
   fournisseur de la signature numérique>
   ```

   Par exemple :

   ```
   [DAC_EXECUTABLE_LIST]

   Count=3

   Item0=?:\Installer\Setup.exe

   Item1=E:\*.exe

   Item2=Trend Micro, Inc.
   ```

5. Enregistrez et fermez le fichier `ofcscan.ini`.

6. Ouvrez la console Web OfficeScan et accédez à **Ordinateurs en réseau** > **Gestion des clients**.

7. Cliquez sur **Enregistrer** pour déployer les listes de programmes vers tous les clients.

Modification des notifications du contrôle des dispositifs

En cas de violation du contrôle des dispositifs, des messages de notification s'affichent sur les points finaux. Si nécessaire, les administrateurs peuvent également modifier le message de notification par défaut.

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.
2. Cliquez sur l'onglet **Violations du contrôle des dispositifs**.
3. Saisissez les messages par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de contrôle des dispositifs

Les clients OfficeScan consignent dans des journaux les accès à des périphériques non autorisés et envoient ces journaux au serveur. Un client qui s'exécute en permanence regroupe les journaux et les envoie toutes les 24 heures par défaut. Dès qu'un client est redémarré, son système vérifie à quel moment les journaux ont été envoyés au serveur pour la dernière fois. Si ce le délai écoulé dépasse 24 heures, ce client envoie les journaux immédiatement.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de contrôle des dispositifs

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité** ou à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Journaux** > **Journaux de contrôle des dispositifs** ou **Afficher les journaux** > **Journaux de contrôle des dispositifs**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Détection d'un accès non autorisé Date/Heure
   - Ordinateur auquel est connecté le périphérique externe ou sur lequel est mappée la ressource réseau
   - Domaine d'ordinateur auquel est connecté le périphérique externe ou sur lequel est mappée la ressource réseau
   - Type de périphérique ou ressource réseau accédés
   - Cible, qui est l'élément accédé sur le périphérique ou la ressource réseau
   - Accédé par, qui spécifie le lieu d'où l'accès a été lancé
   - Autorisations accordées pour la cible
6. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Chapitre 9

Gestion de la protection des données et mise en œuvre de la prévention contre la perte de données

Ce chapitre explique comment installer et activer le module Protection des données et utiliser la fonctionnalité Prévention contre la perte de données.

Sujets abordés dans ce chapitre :

- *Installation de la protection des données à la page 9-2*
- *Licence de protection des données à la page 9-4*
- *Déploiement de la protection des données vers les clients à la page 9-6*
- *À propos de la prévention contre la perte de données à la page 9-9*
- *Stratégies de prévention contre la perte de données à la page 9-11*
- *Notifications de la prévention contre la perte de données à la page 9-55*
- *Journaux de prévention contre la perte de données à la page 9-60*
- *Désinstallation de la protection des données à la page 9-66*

Installation de la protection des données

Le module de protection des données intègre les fonctions suivantes :

- **Prévention contre la perte de données (DLP)** : empêche toute transmission non autorisée d'actifs numériques
- **Contrôle des dispositifs** : Régulation de l'accès aux périphériques externes

Remarque

OfficeScan dispose d'une fonction prête à l'emploi de contrôle des dispositifs, qui régule l'accès aux dispositifs fréquemment utilisés comme les périphériques de stockage USB. Le contrôle des dispositifs, qui fait partie intégrante du module de protection des données, élargit la portée des dispositifs contrôlés. Pour obtenir la liste des dispositifs surveillés, voir *Contrôle des dispositifs à la page 8-2*.

La prévention contre la perte de données et le contrôle des dispositifs sont des fonctionnalités natives OfficeScan mais fournies sous des licences distinctes. Après que vous avez installé le serveur OfficeScan, ces fonctions sont disponibles, mais elles ne sont pas exécutables et ne peuvent pas être déployées vers des clients. L'installation de la protection des données implique le téléchargement d'un fichier depuis le serveur ActiveUpdate (ou depuis une source de mise à jour personnalisée, si définie). Une fois le fichier intégré au serveur OfficeScan, vous pouvez activer la licence de protection de données pour que ses fonctions soient totalement opérationnelles. L'installation et l'activation sont exécutées à partir de **Plug-in Manager**.

Important

Vous n'avez pas besoin d'installer le module Protection des données si le logiciel Trend Micro Data Loss Prevention est déjà installé et qu'il s'exécute aux points finaux.

Le module Protection des données peut être installé sur un IPv6 pur Plug-In Manager. Toutefois, seule la fonction de contrôle des dispositifs peut être déployée sur les clients IPv6 purs. La fonctionnalité Prévention contre la perte de données ne s'exécute pas sur les clients purs IPv6.

Installation de la protection des données

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.

2. Dans l'écran **Plug-in Manager**, accédez à la section **Protection des données OfficeScan** et cliquez sur **Télécharger**.

   La taille du fichier à télécharger s'affiche en regard du bouton **Télécharger**.

   Plug-In Manager stocke le fichier téléchargé dans <*le dossier d'installation du serveur*>`\PCCSRV\Télécharger\Produit`.

   Remarque

   Si Plug-In Manager le téléchargement du fichier n'est pas possible, il est relancé automatiquement après 24 heures. Pour déclencher manuellement le téléchargement du fichier par Plug-In Manager, redémarrez le service OfficeScanPlug-In Manager à partir de Microsoft Management Console.

3. Surveillez la progression du téléchargement.

   Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

   Si vous rencontrez des problèmes lors du téléchargement du fichier, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Journaux de mise à jour du serveur**.

   Une fois le fichier téléchargé par Plug-In Manager, la protection des données OfficeScan s'affiche dans une nouvelle fenêtre.

   Remarque

   Si la protection des données OfficeScan ne s'affiche pas, consultez les causes et les solutions dans la section *Dépannage de Plug-In Manager à la page 14-10*.

4. Pour installer Protection des données OfficeScan immédiatement, cliquez sur **Installer**, ou pour l'installer ultérieurement, exécutez ce qui suit :

   a. Cliquez sur **Installer ultérieurement**.

b. Ouvrez la fenêtre **Plug-in Manager**.

c. Accédez à la section **Protection des données OfficeScan**, puis cliquez sur **Installer**.

5. Lisez attentivement le contrat de licence, puis acceptez ses termes en cliquant sur **Accepter**.

   L'installation démarre.

6. Surveillez la progression de l'installation. Après l'installation, la version de la protection des données OfficeScan s'affiche.

Licence de protection des données

Affichez, activez et renouvelez la licence de protection des données depuis Plug-In Manager.

Obtenez un code d'activation auprès de Trend Micro, puis utilisez-le afin d'activer la licence.

Activation ou renouvellement de la licence de protection des données.

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Dans l'écran **Plug-in Manager**, accédez à la section Protection des données OfficeScan et cliquez sur **Gestion de programme**.
3. Cliquez sur **Nouveau code d'activation**.
4. Entrez le code d'activation.

   Vous pouvez également copier le code d'activation, puis le coller dans n'importe quelle zone de texte.

5. Cliquez sur **Enregistrer**.

Affichage des informations de licence de protection des données

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Dans l'écran **Plug-in Manager**, accédez à la section Protection des données OfficeScan et cliquez sur **Gestion de programme**.
3. Cliquez sur **Afficher les informations de licence**.
4. Consultez les informations suivantes relatives à la licence dans l'écran qui s'ouvre.
   - **État** : affiche « Activé », « Non activé » ou « Expiré ».
   - **Version** : affiche la version « complète » ou la version d'« évaluation ». L'activation à la fois de la version finale et de la version d'évaluation s'affiche uniquement comme « Full ».
   - **Postes** : Affiche le nombre des clients OfficeScan qui peuvent installer le module de protection des données
   - **Date d'expiration du contrat de licence**: Si la protection des données dispose de plusieurs licences, la dernière date d'expiration s'affiche. Par exemple, si les dates d'expiration de la licence sont le 31/12/11 et le 30/06/11, la date qui s'affiche est le 31/12/11.
   - **Code d'activation** : Affiche le code d'activation
   - Messages de rappel : Selon votre version de licence actuelle, la protection des données affiche des messages de rappel quant à la date d'expiration de la licence, soit durant la période de grâce (version finale uniquement), soit lorsque la licence expire.

Remarque

La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro.

Si vous ne renouvelez pas la licence, la prévention contre la perte des données et le contrôle des dispositifs fonctionnent toujours, mais vous n'aurez plus accès au support technique.

5. Cliquez sur **Afficher le détail de la licence en ligne** pour afficher les informations relatives à votre licence sur le site Web de Trend Micro.

6. Pour rafraîchir l'écran avec les dernières informations de licence, cliquez sur **Informations sur la mise à jour**.

Déploiement de la protection des données vers les clients

Déployez le module Protection des données vers les clients OfficeScan après activation de leur licence. Après le déploiement, les clients OfficeScan pourront utiliser la prévention contre la perte de données et le contrôle des dispositifs.

Important

- Par défaut, le module est désactivé sur Windows Server 2003 et Windows Server 2008, pour éviter tout impact sur les performances de la machine hôte. Si vous souhaitez activer le module, surveillez constamment les performances du système et effectuez les actions nécessaires lorsque vous remarquez une baisse de performances.

  Remarque

  Vous pouvez activer et désactiver le module à partir de la console Web. Pour obtenir des informations détaillées, voir *Services du client OfficeScan à la page 13-7*.

- Si le logiciel Trend Micro Data Loss Prevention existe déjà au point final, OfficeScan ne le remplacera pas par le module de protection des données.
- Seul le contrôle des dispositifs peut être déployé sur les clients IPv6 purs. La prévention contre la perte de données ne fonctionne pas sur les clients purs IPv6.
- Les clients en ligne installent le module de protection des données immédiatement. Les clients hors ligne et itinérants installent le module dès qu'ils se connectent en ligne.
- Les utilisateurs doivent redémarrer leurs ordinateurs pour finaliser l'installation des pilotes Prévention contre la perte de données. Informez les utilisateurs qu'un redémarrage anticipé est nécessaire.
- Trend Micro vous recommande d'activer la journalisation du débogage pour pouvoir résoudre les problèmes de déploiement. Pour obtenir des informations détaillées, voir *Journaux de débogage de protection des données à la page 9-65*.

Déploiement du module Protection des données sur des Clients

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence client, vous pouvez :
   - Cliquez sur l'icône du domaine racine ( ) pour déployer le module à tous les clients actuels et futurs.

- sélectionner un domaine spécifique pour déployer le module vers tous les clients existants et à venir associés ;
- sélectionner un client spécifique pour déployer le module uniquement vers ce client.

3. Déployez le module de deux manières différentes :
   - Cliquez sur **Paramètres** > **Paramètres DLP**.
   - Cliquez sur **Paramètres** > **Paramètres de contrôle des dispositifs**.

   Remarque

   Si vous déployez à partir de **Paramètres** > **Paramètres DLP** et si le module Protection des données a été déployé avec succès, les pilotes de prévention contre la perte de données seront installés. Si les pilotes sont correctement installés, un message s'affiche, invitant les utilisateurs à redémarrer leurs ordinateurs pour finaliser l'installation des pilotes.

   Si le message ne s'affiche pas, il peut y avoir des problèmes pour installer les pilotes. Si vous avez activé la journalisation du débogage, vérifiez les journaux de débogage pour en savoir plus sur les problèmes relatifs à l'installation des pilotes.

4. Un message s'affiche, indiquant le nombre de clients pour lesquels le module n'a pas été installé. Cliquez sur **Oui** pour lancer le déploiement.

   Remarque

   Si vous cliquez sur **Non** (ou si le module n'a pas été déployé sur un ou plusieurs clients pour un motif quelconque), le même message s'affiche lorsque vous cliquez à nouveau sur **Paramètres** > **Paramètres DLP** ou **Paramètres** > **Paramètres de contrôle des dispositifs**.

   Les clients commencent à télécharger le module depuis le serveur.

5. Vérifiez si le module a été déployé vers les clients.
   a. Dans l'arborescence du client, sélectionnez un domaine.
   b. Dans la vue de l'arborescence du client, sélectionnez **Affichage de la protection des données** ou **Afficher tout**.

c. Consultez la colonne **État de protection des données**. L'état du déploiement peut être l'un des suivants :

- **En cours d'exécution** : le module a été déployé avec succès et ses fonctionnalités ont été activées.
- **Redémarrage requis**: les pilotes de prévention contre la perte de données n'ont pas été installés car les utilisateurs n'ont pas redémarré leurs ordinateurs. Si les pilotes ne sont pas installés, la prévention contre la perte de données ne pourra pas fonctionner.
- **Arrêté** : Le service du module n'a pas été démarré, ou l'ordinateur cible a été arrêté normalement. Pour démarrer le service de protection de données, accédez à **Ordinateurs en réseau** > **Gestion des clients > Paramètres** > **Paramètres des services complémentaires** et activez les services de protection de données.
- **Installation impossible**: un problème est survenu lors du déploiement du module vers le client. Vous devez redéployer le module à partir de l'arborescence du client.
- **Installation impossible (la prévention contre la perte de données existe déjà)** : Le logiciel Trend Micro Data Loss Prevention existe déjà au point final. OfficeScan ne le remplacera pas par le module Protection des données.
- **Non installé** : Le module n'a pas été déployé vers le client. Ce statut s'affiche si vous choisissez de ne pas déployer le module vers le client, ou si l'état du client est « Hors ligne » ou « Itinérant » pendant le déploiement.

À propos de la prévention contre la perte de données

Les solutions de sécurité classiques sont destinées à empêcher les menaces de sécurité externes d'atteindre le réseau. Dans l'environnement de sécurité actuel, elles s'avèrent incomplètes. Les failles de sécurité sont désormais monnaie courante et exposent les

données sensibles et confidentielles d'une organisation (appelées des actifs numériques) à des entités externes non autorisées. Une faille de sécurité peut résulter d'erreurs ou de négligences des employés internes, de l'externalisation des données, d'ordinateurs volés ou égarés, ou d'attaques malveillantes.

Les violations de données peuvent :

- Porter préjudice à la réputation de la marque
- Diminuer la confiance des clients envers l'organisation
- Entraîner des coûts supplémentaires pour couvrir la réparation et le paiement d'amandes pour violation des règles de conformité
- Mener à la perte d'opportunités commerciales et de chiffre d'affaires lorsque la propriété intellectuelle est volée

Du fait de la fréquence et des effets dramatiques des violations de données, les organisations considèrent dorénavant la protection des actifs numériques comme un composant décisif de leur infrastructure de sécurité.

La prévention contre la perte de données protège les données sensibles de l'entreprise contre toute fuite accidentelle ou délibérée. La prévention contre la perte des données permet ce qui suit :

- Identifiez les informations sensibles exigeant une protection à l'aide d'identificateurs de données
- La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes.
- Le renforcement de la conformité à des normes de confidentialité établies

Avant de pouvoir contrôler une perte potentielle des informations sensibles, vous devez être en mesure de répondre aux questions suivantes :

- Quelles données doivent être protégées des utilisateurs non autorisés ?
- Où se trouvent les données sensibles ?
- Comment sont transmises les données sensibles ?
- Quels sont les utilisateurs autorisés à accéder ou transmettre les données sensibles ?

- Quelle action doit être entreprise en cas de violation de la sécurité ?

Cet audit primordial implique en général plusieurs départements et membres du personnel au courant des informations sensibles de votre entreprise.

Si vous avez déjà défini les informations sensibles et les stratégies de sécurité, vous pouvez commencer à définir les identificateurs de données ainsi que les stratégies d'entreprise.

Stratégies de prévention contre la perte de données

OfficeScan évalue un fichier ou des données par rapport à un ensemble de règles définies dans les stratégies de prévention contre la perte de données. Les stratégies déterminent des fichiers ou des données qui doivent être protégés des transmissions non autorisées et l'action qu'OfficeScan doit effectuer lorsqu'il détecte une transmission.

Remarque

Les transmissions de données entre le serveur OfficeScan et ses clients ne sont pas surveillées.

Vous pouvez configurer les stratégies pour les clients internes et externes. Les administrateurs OfficeScan configurent généralement une stratégie plus stricte pour les clients externes.

Vous pouvez appliquer des stratégies spécifiques à des groupes de clients ou à des clients individuels. Vous pouvez également appliquer une stratégie unique à tous les clients.

Une fois que vous avez déployé les stratégies, les clients utilisent les critères d'emplacement définis dans l'écran **Emplacement de l'ordinateur** (voir *Emplacement de l'ordinateur à la page 13-2*) afin de déterminer leur emplacement et la stratégie à appliquer. Les clients changent de stratégie à chaque fois que l'emplacement change.

Configuration de la stratégie

Définissez les stratégies de prévention contre la perte de données en configurant les paramètres suivants :

TABLEAU 9-1. Paramètres définissant une stratégie de prévention contre de la perte de données

PARAMÈTRES	DESCRIPTION
Identificateurs de données	OfficeScan utilise des identificateurs de données pour identifier les informations sensibles. Les identificateurs comprennent les expressions, les attributs de fichier et les mots-clés.
Modèle	Un modèle de prévention contre la perte de données réunit les identificateurs de données et les opérateurs logiques (Et, Ou, Sauf) pour former des conditions. Seuls les fichiers ou les données qui satisfont à certaines conditions feront l'objet d'une stratégie de prévention contre la perte des données. OfficeScan est fourni avec un ensemble de modèles prédéfinis et vous autorise à créer des modèles personnalisés. Une stratégie de prévention contre la perte de données peut contenir un ou plusieurs modèles. OfficeScan utilise la règle de première correspondance lors de la vérification des modèles. Cela signifie que si un fichier ou des données correspondent aux identificateurs de données d'un modèle, OfficeScan ne vérifiera plus les autres modèles.
Canal	Les canaux sont des entités de transmission d'informations sensibles. OfficeScan prend en charge les canaux de transmission les plus populaires comme les courriers électroniques, les périphériques de stockage amovibles et les applications de messagerie instantanée.
Action	OfficeScan exécute une ou plusieurs actions lorsqu'il détecte une tentative de transmission d'informations sensibles via n'importe quel canal.

Types d'identificateurs de données

Les actifs numériques sont des fichiers et des données qu'une entreprise doit protéger contre les transmissions non autorisées. Vous pouvez définir les actifs numériques à l'aide des identificateurs de données suivants :

- **Expressions** : Données ayant une certaine structure. Pour obtenir des informations détaillées, voir *Expressions à la page 9-13*.
- **Attributs de fichier** : Propriétés d'un fichier, telles que son type ou sa taille. Pour obtenir des informations détaillées, voir *Attributs de fichier à la page 9-18*.
- **Mots-clés** : Liste de mots ou d'expressions particuliers. Pour obtenir des informations détaillées, voir *Mots-clés à la page 9-21*.

Remarque

Il n'est pas possible de supprimer un identificateur de données qui est utilisé dans un modèle DLP. Supprimez le modèle pour pouvoir supprimer l'identificateur de données.

Expressions

Une expression est constituée de données ayant une certaine structure. Par exemple, une carte de crédit possède généralement un numéro à 16 chiffres, présenté sous le format « nnnn-nnnn-nnnn-nnnn », pouvant être localisé lors d'une détection basée sur les expressions.

Vous pouvez utiliser des expressions prédéfinies et personnalisées. Pour obtenir des informations détaillées, voir *Expressions prédéfinies à la page 9-13* et *Expressions personnalisées à la page 9-14*.

Expressions prédéfinies

OfficeScan est fourni avec un ensemble d'expressions prédéfinies. Ces expressions ne peuvent pas être modifiées ou supprimées.

OfficeScan vérifie ces expressions au moyen du processus de correspondance des signatures et d'équations mathématiques. Lorsque OfficeScan fait correspondre des données potentiellement sensibles avec une expression, les données peuvent également être soumises à des vérifications supplémentaires.

Pour obtenir une liste complète d'expressions prédéfinies, accédez à http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Affichage des paramètres des expressions prédéfinies

Remarque

Les expressions prédéfinies ne peuvent pas être modifiées ou supprimées.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur le nom de l'expression.
4. Consultez les paramètres sur l'écran qui s'affiche.

Expressions personnalisées

Si aucune des expressions prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Les expressions constituent un outil puissant de correspondance de chaînes. Avant de procéder à la création d'expressions, vérifiez que vous maîtrisez la syntaxe des expressions. Les expressions mal formulées peuvent avoir un impact conséquent sur les performances.

Lorsque vous créez des expressions :

- Reportez-vous aux expressions prédéfinies pour savoir comment définir une expression valide. Par exemple, si vous créez une expression qui comprend une date, vous pouvez vous référer aux expressions précédées de «Date».
- Remarque : OfficeScan respecte les formats d'expression définis dans la bibliothèque Perl Compatible Regular Expressions (PCRE). Pour plus d'informations sur PCRE, visitez le site Web suivant :

http://www.pcre.org/

- Commencez par des expressions simples. Modifiez les expressions si celles-ci déclenchent de fausses alertes, ou ajustez-les pour améliorer les détections.

Lors de la création d'expressions, plusieurs critères sont à votre disposition. Une expression doit correspondre aux critères que vous avez choisis pour qu'OfficeScan puisse la soumettre à une stratégie de prévention contre la perte de données. Pour plus de détails sur les différentes actions, reportez-vous à *Critères applicables aux expressions personnalisées à la page 9-15*.

Critères applicables aux expressions personnalisées

TABLEAU 9-2. Options de critères pour des expressions personnalisées

CRITÈRES	RÈGLE	EXEMPLE
Aucune	Aucune	Tous - Noms du Bureau du recensement des États-Unis Expression : [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Caractères spécifiques	Une expression doit intégrer les caractères que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	États-Unis - Numéro de routage ABA Expression : [^\d]([0123678]\d{8})[^\d] Caractères : 0123456789 Nombre de caractères minimal : 9 Nombre de caractères maximal : 9

CRITÈRES	RÈGLE	EXEMPLE
Suffixe	Le suffixe correspond au dernier segment d'une expression. Un suffixe doit compter un certain nombre de caractères et inclure ceux que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	Tous - Adresse de domicile Expression : \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] Caractères pour le suffixe : 0123456789- Nombre de caractères : 5 Nombre de caractères minimal dans l'expression : 25 Nombre de caractères maximal dans l'expression : 80
Un seul caractère de séparation	Une expression doit comporter deux segments séparés par un caractère. Le caractère doit avoir une longueur d'un octet. De plus, le nombre de caractères situés à gauche du séparateur doit être compris dans les limites minimale et maximale définies. Le nombre de caractères situés à droite ne doit pas dépasser la limite maximale.	Tous - Adresse électronique Expression : [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] Séparateur : @ Nombre de caractères minimal à gauche : 3 Nombre de caractères maximal à gauche : 15 Nombre de caractères maximal à droite : 30

Création d'une expression personnalisée

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **expression**.

3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

4. Entrez un nom pour l'expression. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

5. Saisissez une description ne dépassant pas 256 octets.

6. Saisissez l'expression et indiquez si celle-ci respecte la casse.

7. Saisissez les données affichées.

   Par exemple, si vous créez une expression pour des numéros ID, saisissez un exemple de numéro ID. Ces données sont utilisées à des fins de référence uniquement et ne figureront pas sur le produit.

8. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère (voir *Critères applicables aux expressions personnalisées à la page 9-15*) :

   - Aucune
   - Caractères spécifiques
   - Suffixe
   - Un seul caractère de séparation

9. Testez l'expression avec des données réelles.

   Par exemple, si l'expression s'applique à un ID national, entrez un numéro ID valide dans la zone de texte **Données de test**, cliquez sur **Tester**, puis vérifiez le résultat.

10. Cliquez sur **Enregistrer** si vous êtes satisfait du résultat.

Remarque

Enregistrez les paramètres uniquement si le test a réussi. Une expression qui ne détecte aucune donnée consomme les ressources du système inutilement et peut avoir une influence négative sur les performances.

11. Un message s'affiche vous rappelant de déployer les paramètres vers les clients. Cliquez sur **Fermer**.

12. Cliquez sur **Appliquer à tous les clients** pour revenir à l'écran **Identificateurs de données pour la prévention contre la perte de données**.

Importation d'une expression personnalisée

Si le formatage du fichier `.dat` contenant les expressions est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les expressions à partir du serveur OfficeScan actif ou à partir de tout autre serveur OfficeScan.

Remarque

Les fichiers d'expression `.dat` générés par cette version d'OfficeScan ne sont pas compatibles avec les versions précédentes.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **expression**.

3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les expressions.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une expression à importer existe déjà, elle sera ignorée.

5. Cliquez sur **Appliquer à tous les clients**.

Attributs de fichier

Les attributs de fichier sont des propriétés spécifiques à un fichier. Vous pouvez utiliser deux attributs de fichier lorsque vous définissez des identificateurs de données, à savoir le type de fichier et la taille de fichier. Par exemple, une entreprise de développement de logiciels souhaitera peut-être limiter le partage du programme d'installation d'un logiciel

d'entreprise aux membres du service de recherche & développement, lesquels sont chargés de développer et tester le logiciel. Dans ce cas, l'administrateur OfficeScan peut créer une stratégie qui bloque la transmission des fichiers exécutables de 10 à 40 Mo vers l'ensemble des départements, à l'exception de celui de la recherche et du développement.

Les attributs de fichier ne permettent pas, en tant que tels, d'identifier les fichiers sensibles. Si nous reprenons l'exemple cité dans cette rubrique, les programmes d'installation de logiciels tiers partagés par d'autres départements risquent d'être bloqués. Par conséquent, Trend Micro recommande d'associer les attributs de fichier à d'autres identificateurs de données pour la prévention contre la perte de données, ce, pour permettre une détection plus ciblée des fichiers sensibles.

Pour obtenir une liste complète d'expressions prédéfinies, voir http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Création d'une liste d'attributs de fichier

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **attribut de fichier**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Saisissez un nom pour la liste d'attributs de fichier. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets.
6. Sélectionnez vos véritables types de fichiers favoris.
7. Si un type de fichier que vous souhaitez inclure n'est pas répertorié, sélectionnez **Extensions de fichier** et entrez l'extension du type de fichier. OfficeScan vérifie les fichiers contenant l'extension spécifiée mais pas le véritable type de fichier. Directives à suivre lorsque vous saisissez des extensions de fichiers :

- Chaque extension doit commencer par un astérisque (*), suivi d'un point (.) et ensuite de l'extension. L'astérisque est un caractère générique qui représente un nom réel de fichier. Par exemple, `*.pol` correspond à `12345.pol` et `test.pol`.
- Vous pouvez inclure des caractères génériques dans les extensions. Utilisez un point d'interrogation (?) pour représenter un seul caractère et un astérisque (*) pour deux caractères ou plus. Voir les exemples suivants :

  - `*.*m` correspond aux fichiers suivants : `ABC.dem`, `ABC.prm`, `ABC.sdcm`

  - `*.m*r` correspond aux fichiers suivants : `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

  - `*.fm?` correspond aux fichiers suivants : `ABC.fme`, `ABC.fml`, `ABC.fmp`
- Faites attention si vous utilisez un astérisque à la fin d'une extension car il peut correspondre à des parties de noms de fichiers et à une extension sans rapport. Par exemple : `*.do*` correspond à `abc.doctor_john.jpg` et `abc.donor12.pdf`.
- Utilisez les points-virgules (;) pour séparer les extensions de fichier. Il n'est pas nécessaire d'ajouter un espace après un point-virgule.

8. Entrez les tailles de fichier minimale et maximale en octets. Les valeurs doivent être des entiers non nuls.
9. Cliquez sur **Enregistrer**.
10. Un message s'affiche vous rappelant de déployer les paramètres vers les clients. Cliquez sur **Fermer**.
11. Cliquez sur **Appliquer à tous les clients** pour revenir à l'écran **Identificateurs de données pour la prévention contre la perte de données**.

Importation d'une liste d'attributs de fichier

Si le formatage du fichier `.dat` contenant les listes d'attributs de fichier est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les listes d'attributs de fichier à partir du serveur OfficeScan actif ou à partir de tout autre serveur OfficeScan.

Remarque

Les fichiers d'attributs `.dat` générés par cette version d'OfficeScan ne sont pas compatibles avec les versions précédentes.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **attribut de fichier**.
3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les listes d'attributs de fichier.
4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste d'attributs de fichier à importer existe déjà, elle sera ignorée.
5. Cliquez sur **Appliquer à tous les clients**.

Mots-clés

Les mots-clés sont des expressions ou des mots spéciaux. Vous pouvez ajouter des mots-clés de la même famille à une liste de mots-clés afin d'identifier un certain nombre de données spécifiques. Par exemple, «pronostic», «groupe sanguin», «vaccination» et «médecin» sont des mots-clés pouvant apparaître dans un certificat médical. Si vous souhaitez éviter la transmission de fichiers contenant des certificats médicaux, vous pouvez utiliser ces mots-clés dans une stratégie de prévention contre la perte de données, puis configurer OfficeScan de manière à bloquer les fichiers contenant ces mots-clés.

Les mots habituellement utilisés peuvent être associés afin de former des mots-clés significatifs. Par exemple, «end», «read», «if» et «at» peuvent être associés pour former des mots-clés présents dans du code source, tels que «END-IF», «END-READ» et «AT END».

Vous pouvez utiliser des listes de mots-clés prédéfinies et personnalisées. Pour obtenir des informations détaillées, voir *Listes de mots-clés prédéfinies à la page 9-22* et *Listes de mots-clés personnalisées à la page 9-23*.

Listes de mots-clés prédéfinies

OfficeScan est fourni avec un ensemble de listes de mots-clés prédéfinies. Ces listes de mots-clés ne peuvent pas être modifiées ou supprimées. Chaque liste a ses propres conditions intégrées qui déterminent si le modèle doit déclencher une violation de stratégie.

Pour plus d'informations sur les listes de mots-clés prédéfinies dans OfficeScan, voir http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Fonctionnement des listes de mots-clés

Condition de nombre de mots-clés

Chaque liste de mots-clés contient une condition qui requiert qu'un certain nombre de mots-clés existe dans un document avant que la liste ne déclenche une violation.

La condition du nombre de mots-clés contient les valeurs suivantes :

- **Tous** : Tous les mots-clés de la liste doivent exister dans le document.
- **Tout** : N'importe quel mot-clé de la liste doit exister dans le document.
- **Nombre spécifique** : Le document doit comporter au moins le nombre spécifié de mots-clés. S'il y a plus de mots-clés dans le document que le nombre spécifié, une violation se déclenche.

Condition de distance

Certaines des listes contiennent une condition de « distance » pour savoir si une violation est présente. « Distance » se réfère au nombre de caractères existant entre le premier caractère d'un mot clé et le premier caractère d'un autre mot-clé. L'entrée suivante peut servir d'exemple :

P**rénom :_John_ N**om :_Smith_

La liste des **Formulaires - Prénom, nom** comporte une condition de « distance » de cinquante (50) et les champs de formulaire couramment utilisés de « Prénom » et « Nom ». Dans l'exemple ci-dessus, une violation se déclenchera car le nombre de caractères entre le « P » et le « N » de « nom » est égal à dix-huit (18).

Voici un exemple d'entrée qui ne déclenchera pas de violation :

Le P**rénom de notre nouvel employé de Suisse est John. Son N**om est Smith.

Dans cet exemple, le nombre de caractères entre le « p » de « prénom » et le « n » de « nom » est soixante et un (61). Cela dépasse le seuil de distance et ne déclenche pas de violation.

Listes de mots-clés personnalisées

Si aucune des listes de mots-clés prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Lors de la configuration d'une liste de mots-clés, plusieurs critères sont à votre disposition. Une liste de mots-clés doit correspondre aux critères que vous avez choisis avant qu'OfficeScan puisse la soumettre à une stratégie de prévention contre la perte des données. Pour chaque liste de mots-clés, choisissez l'un des critères suivants :

- **N'importe quel mot-clé**
- **Tous les mots-clés**
- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

Pour plus d'informations concernant les règles de critères, voir *Critères des listes personnalisées de mots-clés à la page 9-23*.

Critères des listes personnalisées de mots-clés

TABLEAU 9-3. Critères pour une liste de mots-clés

CRITÈRES	RÈGLE
N'importe quel mot-clé	Un fichier doit contenir au moins un mot-clé de la liste.

CRITÈRES	RÈGLE
Tous les mots-clés	Le fichier doit contenir tous les mots-clés de la liste.
Tous les mots-clés de <x> caractères maximum	Le fichier doit contenir tous les mots-clés de la liste. En outre, toute paire de mots-clés doit différer au plus de <x> caractères l'une par rapport à l'autre. Par exemple, vos 3 mots-clés sont WEB, DISK et USB, et le nombre de caractères que vous avez indiqué est 20. Si OfficeScan détecte tous les mots-clés dans l'ordre DISK, WEB et USB, le nombre de caractères du « D » (de DISK) au « W » (de WEB) et du « W » au « U » (de USB) doit être inférieur ou égal à 20 caractères. Les données suivantes correspondent au critère : DISK####WEB############USB Les données suivantes ne correspondent pas au critère : DISK**********WEB****USB(23 caractères entre le « D » et le « W ») Lorsque vous déterminez le nombre de caractères, gardez à l'esprit qu'un petit nombre, comme 10, permettra généralement un scan plus rapide, mais couvrira uniquement une zone relativement restreinte. La plage de détection des données sensibles risque donc d'être limitée, en particulier pour les fichiers volumineux. Plus le nombre est grand, plus la zone couverte est importante et plus la durée du scan est longue.

CRITÈRES	RÈGLE
Le score combiné des mots-clés dépasse le seuil	Un fichier doit contenir un ou plusieurs mots-clés de la liste. Si un seul mot-clé est détecté, son score doit être supérieur au seuil défini. Si plusieurs mots-clés sont détectés, leur score combiné doit être supérieur au seuil défini. Attribuez à chaque mot-clé un score de 1 à 10. Un terme ou une phrase à haute confidentialité, comme « augmentation des salaires » pour le département des ressources humaines, doit avoir un score relativement élevé. Les termes ou les phrases qui, en elles-mêmes, n'ont pas de poids significatif peuvent avoir des scores plus faibles. Pensez aux scores que vous avez attribués aux mots-clés lorsque vous configurez le seuil. Par exemple, si vous avez cinq mots-clés, dont trois avec une priorité élevée, le seuil peut être égal ou inférieur au score combiné des trois mots-clés à priorité élevée. Cela signifie que la détection de ces trois mots-clés est suffisante pour classer le fichier comme étant sensible.

Création d'une liste Mot-clé

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **Mot-clé**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Entrez un nom pour la liste de mots-clés. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets.
6. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère :

   - **N'importe quel mot-clé**

- **Tous les mots-clés**
- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

7. Pour ajouter manuellement des mots-clés à la liste :

   a. Saisissez un mot-clé d'une longueur de 3 à 40 octets et indiquez s'il respecte la casse.

   b. Cliquez sur **Ajouter**.

8. Pour ajouter des mots-clés à l'aide de l'option d'« importation » :

   Remarque

   Si le formatage du fichier .csv contenant les mots-clés est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les mots-clés à partir du serveur OfficeScan actif ou à partir de tout autre serveur OfficeScan.

   a. Cliquez sur **Importer** et identifiez le fichier `.csv` contenant les mots-clés.

   b. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un mot-clé à importer existe déjà dans la liste, il sera ignoré.

9. Pour supprimer des mots-clés, sélectionnez-les puis cliquez sur **Supprimer**.

10. Pour exporter des mots-clés :

    Remarque

    Utilisez la fonctionnalité « exporter » pour sauvegarder les mots-clés ou les importer sur un autre serveur OfficeScan. Tous les mots-clés de la liste seront exportés. Il n'est pas possible d'exporter un mot-clé individuel.

    a. Cliquez sur **Exporter**.

    b. Enregistrez le fichier `.csv` obtenu à l'emplacement de votre choix.

11. Cliquez sur **Enregistrer**.

12. Un message s'affiche vous rappelant de déployer les paramètres vers les clients. Cliquez sur **Fermer**.

13. Cliquez sur **Appliquer à tous les clients** pour revenir à l'écran **Identificateurs de données pour la prévention contre la perte de données**.

Importation d'une liste Mot-clé

Utilisez cette option si vous avez un fichier `.dat` correctement formaté et contenant les listes de mots-clés. Pour générer le fichier, vous pouvez exporter les listes de mots-clés à partir du serveur OfficeScan actif ou à partir de tout autre serveur OfficeScan.

Remarque

Les fichiers de liste `.dat` de mot-clé générés par cette version d'OfficeScan ne sont pas compatibles avec les versions précédentes.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **Mot-clé**.

3. Cliquez sur **Importer** et identifiez le fichier `.dat` contenant les listes de mots-clés.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste de mots-clés à importer existe déjà, elle sera ignorée.

5. Cliquez sur **Appliquer à tous les clients**.

Modèles de prévention contre la perte de données

Un modèle DLP réunit les identificateurs de données et les opérateurs logiques (Et, Ou, Sauf) pour former des conditions. Seuls les fichiers ou les données qui satisfont à certaines conditions feront l'objet d'une stratégie de prévention contre la perte des données.

Par exemple, un fichier doit être un fichier Microsoft Word (attribut de fichier) ET doit contenir certains termes légaux (mots-clés) ET doit contenir des numéros d'identification (expressions) afin de devenir une stratégie de « Contrats de travail ». Cette stratégie autorise le personnel des Ressources humaines à imprimer le fichier afin que cette copie soit signée par un employé. La transmission par le biais de tous les autres canaux possibles, tels que le courrier électronique, est bloquée.

Vous pouvez créer vos propres modèles si vous avez configuré des identificateurs de données. Vous pouvez également utiliser des modèles prédéfinis. Pour obtenir des informations détaillées, voir *Modèles DLP personnalisés à la page 9-29* et *Modèles DLP prédéfinis à la page 9-28*.

Remarque

Il n'est pas possible de supprimer un modèle utilisé dans une stratégie de prévention contre la perte des données. Supprimez le modèle de la stratégie pour pouvoir la supprimer.

Modèles DLP prédéfinis

OfficeScan est fourni avec un ensemble de modèles prédéfinis que vous pouvez utiliser afin de répondre à diverses normes de contrôle. Ces modèles ne peuvent pas être modifiés ou supprimés.

- **GLBA** : Loi Gramm-Leach-Billey Act
- **HIPAA** : Loi Health Insurance Portability and Accountability Act
- **PCI-DSS** : Norme de sécurité des données pour l'industrie des cartes de paiement
- **SB-1386**: Loi n°1386 du Sénat américain
- **US PII** : Données d'identification personnelles des Etats-Unis

Pour obtenir une liste plus détaillée sur tous les modèles prédéfinis, avec des exemples de données sous protection, voir http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Modèles DLP personnalisés

Créez vos propres modèles si vous avez configuré les identificateurs de données. Un modèle réunit des identificateurs de données et des opérateurs logiques (Et, Ou, Sauf) pour former des déclarations de condition.

Pour plus d'informations et d'exemples sur le fonctionnement des déclarations de condition et des opérateurs logiques, voir *Conditions et opérateurs logiques à la page 9-29*.

Conditions et opérateurs logiques

OfficeScan évalue les instructions de gauche à droite. Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus.

Reportez-vous aux exemples dans le tableau ci-dessous.

TABLEAU 9-4. Exemples de conditions

CONDITION	INTERPRÉTATION ET EXEMPLE
[Identificateur de données 1] **et** [Identificateur de données 2] **sauf** [Identificateur de données 3]	Un fichier doit satisfaire [Identificateur de données 1] et [Identificateur de données 2], mais pas [Identificateur de données 3]. Par exemple : Un fichier doit être [au format Adobe PDF] et doit contenir [une adresse e-mail], mais ne doit pas contenir [tous les mots-clés de la liste].
[Identificateur de données 1] **ou** [Identificateur de données 2]	Un fichier doit safisfaire [Identificateur de données 1] ou [Identificateur de données 2]. Par exemple : Un fichier doit être [un document Adobe PDF] ou [un document Microsoft Word].
Sauf [Identificateur de données 1]	Un fichier ne doit pas satisfaire [Identificateur de données 1]. Par exemple : Un fichier ne doit pas être [un fichier multimédia].

Comme illustré dans le dernier exemple du tableau, le premier identificateur de données de la déclaration de condition peut être associé à l'opérateur « sauf » si un fichier ne satisfait pas tous les identificateurs de données dans la décalaration. Cependant, dans la plupart des cas, le premier identificateur de données ne comporte pas d'opérateur.

Création d'un modèle

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **modèles**.
2. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
3. Entrez un nom pour le modèle. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
4. Saisissez une description ne dépassant pas 256 octets.
5. Sélectionnez des identificateurs de données puis cliquez sur l'icône « Ajouter ».

   Lorsque vous sélectionnez des définitions :

   - Sélectionnez plusieurs entrées en appuyant et en maintenant la touche **CTRL**, puis en sélectionnant les identificateurs de données.
   - Si vous recherchez une définition spécifique, utilisez la fonction de recherche. Vous pouvez saisir le nom complet ou partiel de l'identitificateur de données.
   - Chaque modèle peut contenir au maximum 30 identificateurs de données.
6. Pour créer une nouvelle expression, cliquez sur **expressions** puis sur **Ajouter une nouvelle expression**. Dans l'écran qui s'affiche, configurez les paramètres de l'expression.
7. Pour créer une nouvelle liste d'attributs, cliquez sur **attributs de fichier** puis sur **Ajouter un nouvel attribut de fichier**. Dans l'écran qui s'affiche, configurez les paramètres de la liste d'attributs de fichier.

8. Pour créer une nouvelle liste de mots-clés, cliquez sur **Mots-clés** puis sur **Ajouter un nouveau mot-clé**. Dans l'écran qui s'affiche, configurez les paramètres de la liste de mots-clés.

9. Si vous avez sélectionné une expression, saisissez le nombre d'occurrences, c'est-à-dire le nombre de fois qu'une expression doit se produire avant qu'OfficeScan ne la soumette à une stratégie de prévention contre la perte des données.

10. Choisissez un opérateur logique pour chaque définition.

Remarque

Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus. Pour des exemples d'utilisation correcte, voir *Conditions et opérateurs logiques à la page 9-29*.

11. Pour supprimer un identificateur de données de la liste d'identificateurs sélectionnés, cliquez sur l'icône « corbeille ».

12. Sous **Aperçu**, vérifiez la condition et effectuez des changements s'il ne s'agit pas de la condition souhaitée.

13. Cliquez sur **Enregistrer**.

14. Un message s'affiche vous rappelant de déployer les paramètres vers les clients. Cliquez sur **Fermer**.

15. De retour sur l'écran des **Modèles DLP**, cliquez sur **Appliquer à tous les clients**.

Importation d'un modèle

Utilisez cette option si vous disposez d'un fichier `.dat`correctement formaté comprenant les modèles. Pour générer le fichier, vous pouvez exporter les modèles à partir du serveur OfficeScan actif ou à partir de tout autre serveur OfficeScan.

Remarque

Pour importer des modèles DLP d'OfficeScan 10.6, importez les identificateurs de données associés (préalablement nommés Définitions). OfficeScan ne peut pas importer les modèles qui ne sont pas associés à leurs identificateurs de données.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Prévention contre la perte de données** > **modèles**.
2. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les modèles.
3. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un modèle à importer existe déjà, il sera ignoré.
4. Cliquez sur **Appliquer à tous les clients**.

Canaux DLP

Les utilisateurs peuvent transmettre des informations sensibles par le biais de différents canaux. OfficeScan peut contrôler les canaux suivants :

- **Canaux réseau** : les informations sensibles sont transmises selon des protocoles réseau tels que HTTP et FTP.
- **Canaux système et application** : les informations sensibles sont transmises à l'aide d'applications et de périphériques d'un ordinateur local.

Canaux réseau

OfficeScan peut contrôler les transmissions de données via les canaux réseau suivants :

- Clients de messagerie
- FTP
- HTTP et HTTPS
- Applications de messagerie instantanée
- Protocole SMB
- Webmail

Pour déterminer les transmissions de données à contrôler, OfficeScan vérifie l'étendue de transmission. Vous devez la configurer. En fonction de l'étendue sélectionnée, OfficeScan contrôlera toutes les transmissions de données ou uniquement les transmissions effectuées en dehors du réseau local (LAN). Pour plus d'informations sur l'étendue des transmissions, voir *Étendue et cibles de transmission pour les canaux réseau à la page 9-37*.

Clients de messagerie

OfficeScan contrôle les e-mails transmis via divers clients de messagerie. OfficeScan vérifie que l'objet, le corps et les pièces jointes du message ne contiennent pas d'identificateurs de données. Pour obtenir la liste des clients de messagerie pris en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Le contrôle s'effectue lorsqu'un utilisateur tente d'envoyer un e-mail. Si l'e-mail contient des identificateurs de données, OfficeScan l'autorise ou le bloque.

Vous pouvez définir les domaines de messagerie internes contrôlés et non contrôlés.

- **Domaines de messagerie contrôlés** : Quand OfficeScan détecte un courrier électronique transmis à un domaine contrôlé, il vérifie l'action définie par la stratégie. Selon l'action définie, la transmission est autorisée ou bloquée.

  Remarque

  Si vous définissez les clients de messagerie comme des canaux contrôlés, un courrier électronique doit correspondre à une stratégie pour être contrôlé. Par contre, un courrier électronique envoyé à un domaine de messagerie contrôlé est automatiquement vérifié, même s'il ne correspond pas à une stratégie.

- **Domaines de messagerie non contrôlés** : OfficeScan autorise immédiatement la transmission d'e-mails envoyés à des domaines non contrôlés.

Remarque

Des transmissions de données effectuées vers des domaines de messagerie non contrôlés et vers des domaines de messagerie contrôlés pour lesquels l'action est définie sur « Contrôler» ont le même résultat, à savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les domaines de messagerie non contrôlés, OfficeScan n'enregistre pas la transmission alors que pour les domaines de messagerie contrôlés, la transmission est toujours enregistrée.

Spécifiez des domaines en utilisant l'un des formats suivants en prenant soin de séparer les domaines par des virgules :

- format X400, tel que /O=Trend/OU=USA, /O=Trend/OU=China
- Domaines de messagerie, comme example.com

Pour les e-mails envoyés via le protocole SMTP, OfficeScan vérifie si le serveur SMTP cible se trouve dans les listes suivantes :

1. Cibles contrôlées
2. Cibles non contrôlées

Remarque

Pour plus d'informations sur les cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 9-39*.

3. Domaines de messagerie contrôlés
4. Domaines de messagerie non contrôlés

Cela signifie que si un courrier électronique est envoyé vers un serveur SMTP se trouvant dans la liste des cibles contrôlées, le courrier est vérifié. Si le serveur SMTP ne se trouve pas dans la liste des cibles contrôlées, OfficeScan vérifie les autres listes.

Pour les courriers électroniques envoyés via d'autres protocoles, OfficeScan ne vérifie que les listes suivantes :

1. Domaines de messagerie contrôlés
2. Domaines de messagerie non contrôlés

FTP

Lorsqu'OfficeScan détecte qu'un client FTP tente de charger des fichiers sur un serveur FTP, il vérifie que les fichiers ne contiennent pas d'identificateurs de données. Aucun fichier n'a été chargé jusqu'à présent. En fonction de la stratégie de prévention contre la perte de données, OfficeScan autorise ou bloque le téléchargement.

Lorsque vous configurez une stratégie qui bloque les chargements de fichiers, tenez compte de ce qui suit :

- Lorsqu'OfficeScan bloque un téléchargement, certains clients FTP tenteront de charger de nouveau les fichiers. Dans ce cas, OfficeScan met fin au client FTP pour empêcher les nouvelles tentatives de téléchargement. Les utilisateurs ne reçoivent pas de notification après l'interruption du client FTP. Informez-les de la situation lorsque vous mettez en œuvre vos stratégies de prévention contre la perte de données.
- Si un fichier à charger écrase un fichier du serveur FTP, le fichier du serveur FTP peut être supprimé.

Pour obtenir la liste des clients FTP pris en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

HTTP et HTTPS

OfficeScan contrôle les données à transmettre via HTTP et HTTPS. Pour HTTPS, OfficeScan vérifie les données avant qu'elles ne soient encodées et transmises.

Pour obtenir la liste des navigateurs Web et des applications pris en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Applications de messagerie instantanée

OfficeScan contrôle les messages et les fichiers que les utilisateurs envoient via les applications de messagerie instantanée. Les messages et les fichiers reçus par les utilisateurs ne sont pas contrôlés.

Pour obtenir la liste des applications de messagerie instantanée prises en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Lorsque OfficeScan bloque un message ou un fichier envoyé via AOL Instant Messenger, MSN, Windows Messenger ou Windows Live Messenger, il met également fin à l'application. Si OfficeScan ne ferme pas l'application, celle-ci ne répondra plus et les utilisateurs devront tout de même y mettre fin. Les utilisateurs ne reçoivent pas de notification après la fermeture de l'application. Informez-les de la situation lorsque vous mettez en œuvre vos stratégies de prévention contre la perte de données.

Protocole SMB

OfficeScan contrôle les transmissions de données via le protocole SMB (Server Message Block), qui facilite l'accès aux fichiers partagés. Lorsqu'un autre utilisateur tente de copier ou de lire un fichier partagé par un autre utilisateur, OfficeScan vérifie si le fichier est ou contient un identificateur de données, puis autorise ou bloque l'opération.

Remarque

L'action Contrôle des dispositifs est prioritaire par rapport à l'action de la prévention contre la perte de données. Par exemple, si le contrôle des dispositifs n'autorise pas le déplacement de fichiers sur des lecteurs réseau mappés, la transmission de données sensibles n'aura pas lieu même si la prévention contre la perte de données l'autorise. Pour plus d'informations concernant les actions de contrôle des dispositifs, voir *Autorisations pour les périphériques de stockage à la page 8-3*.

Pour obtenir la liste des applications qu'OfficeScan contrôle pour l'accès aux fichiers partagés, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Webmail

Les services de messagerie Web transmettent les données via HTTP. Si OfficeScan détecte des données sortant des dispositifs pris en charge, il vérifie les données à la recherche d'identificateurs de données.

Pour obtenir la liste des services de messagerie Web pris en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Étendue et cibles de transmission pour les canaux réseau

L'étendue et les cibles de transmission définissent les transmissions de données sur les canaux réseau qu'OfficeScan doit contrôler. Pour les transmissions qui doivent être contrôlées, OfficeScan vérifie la présence d'identificateurs de données avant d'autoriser ou de bloquer la transmission. Pour les transmissions qui ne doivent pas être contrôlées, OfficeScan ne vérifie pas la présence d'identificateurs de données et autorise directement la transmission.

Étendue de transmission : Toutes les transmissions

OfficeScan contrôle les données transmises hors de l'ordinateur hôte.

Remarque

Trend Micro vous recommande de choisir cette étendue pour les clients externes.

Si vous ne souhaitez pas contrôler les transmissions de données vers certaines cibles hors de l'ordinateur hôte, définissez les points suivants :

- **Cibles non contrôlées**: OfficeScan ne contrôle pas les données transmises vers ces cibles.

  Remarque

  Des transmissions de données effectuées vers des cibles non contrôlées et vers des cibles contrôlées pour lesquelles l'action est définie sur « Contrôler » ont le même résultat, à savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les cibles non contrôlées, OfficeScan n'enregistre pas la transmission alors que pour les cibles contrôlées, la transmission est toujours enregistrée.

- **Cibles contrôlées**: il s'agit de cibles spécifiques, au sein des cibles non contrôlées, qui doivent être contrôlées. Les cibles contrôlées sont :
  - facultatives si vous avez défini des cibles non contrôlées.
  - non configurables si vous n'avez pas défini de cibles non contrôlées.

Par exemple :

Les adresses IP suivantes sont attribuées au département juridique de votre entreprise :

- 10.201.168.1 à 10.201.168.25

Vous créez une stratégie qui contrôle la transmission des contrats de travail vers tous les employés à l'exception du personnel travaillant à plein-temps dans le département juridique. Vous devez donc sélectionner **Toutes les transmissions** comme étendue de transmission et ensuite :

Option n°1 :

1. Ajouter 10.201.168.1 à 10.201.168.25 aux cibles non contrôlées.
2. Ajouter les adresses IP du personnel travaillant à temps partiel dans le département juridique aux cibles contrôlées. Il y aurait 3 adresses IP : 10.201.168.21 à 10.201.168.23.

Option n°2:

Ajouter les adresses IP du personnel travaillant à temps plein dans le département juridique aux cibles non contrôlées.

- 10.201.168.1-10.201.168.20
- 10.201.168.24-10.201.168.25

Pour obtenir les directives sur la manière de définir des cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 9-39*.

Étendue de transmission : uniquement les transmissions hors du réseau local

OfficeScan contrôle les données transmises vers une cible hors du réseau local (LAN).

Remarque

Trend Micro vous recommande de choisir cette étendue pour les clients internes.

«Réseau» se rapporte à l'entreprise ou au réseau local. Le réseau actuel (adresse IP du point final et masque de réseau) et les adresses IP privées standard suivantes sont comprises :

- Classe A : 10.0.0.0 à 10.255.255.255

- Classe B : 172.16.0.0 à 172.31.255.255
- Classe C : 192.168.0.0 à 192.168.255.255

Si vous sélectionnez cette étendue de transmission, vous pouvez définir ce qui suit :

- **Cibles non contrôlées**: cibles situées hors du réseau local que vous considérez comme inoffensives et qui ne doivent donc pas être contrôlées.

Remarque

Des transmissions de données effectuées vers des cibles non contrôlées et vers des cibles contrôlées pour lesquelles l'action est définie sur « Contrôler » ont le même résultat, à savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les cibles non contrôlées, OfficeScan n'enregistre pas la transmission alors que pour les cibles contrôlées, la transmission est toujours enregistrée.

- **Cibles contrôlées**: cibles du réseau local que vous souhaitez contrôler.

Pour obtenir les directives sur la manière de définir des cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 9-39*.

Définition des cibles contrôlées et non contrôlées

Suivez ces directives lorsque vous définissez des cibles contrôlées et non contrôlées :

1. Définissez chaque cible selon :
   - Une adresse IP ou une plage d'adresses
   - Nom de l'hôte
   - Nom de domaine complet (FQDN ou Fully Qualified Domain Name)
   - Adresse réseau et masque de sous-réseau, tel que 10.1.1.1/32

Remarque

Pour le masque de sous-réseau, OfficeScan ne prend en charge que le port de type CIDR (Classless Inter-Domain Routing). Cela signifie que vous ne pouvez entrer qu'un nombre comme 32 au lieu de 255.255.255.0.

2. Pour des canaux cibles spécifiques, incluez les numéros de port par défaut de ces canaux ou les numéros de port définis par l'entreprise. Par exemple, port 21 est typiquement relié au trafic FTP, port 80 à HTTP et port 443 à HTTPS. Utilisez deux points (:) pour séparer la cible des numéros de ports.

3. Vous pouvez également inclure les plages de ports. Pour inclure tous les ports, ignorez la plage de ports.

   Ci-dessous vous trouverez quelques exemples de cibles avec des numéros de port et des plages de ports :

   - 10.1.1.1:80
   - host :5-20
   - host.domain.com:20
   - 10.1.1.1/32:20

4. Séparez les cibles par des virgules.

Résoudre des conflits

Si les paramètres d'étendue de transmission, de cibles contrôlées et non contrôlées entrent en conflit, OfficeScan applique les priorités suivantes de la plus haute à la plus basse :

- Cibles contrôlées
- Cibles non contrôlées
- Étendue de transmission

Canaux système et application

OfficeScan peut contrôler les canaux système et application suivants :

- Enregistreurs de données (CD/DVD)
- Applications Peer-to-Peer
- Chiffrement PGP
- Imprimante

- Stockage amovible
- Logiciel de synchronisation (ActiveSync)
- Presse-papiers Windows

Enregistreurs de données (CD/DVD)

OfficeScan contrôle les données enregistrées sur un CD ou un DVD. Pour une liste des dispositifs et logiciels d'enregistrement de données pris en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Lorsque OfficeScan détecte une demande de «gravure» lancée par l'un de ces dispositifs ou logiciels pris en charge et que l'action est «Ignorer », l'enregistrement des données es effectué. Si l'action définie est « Bloquer », OfficeScan vérifie si les fichiers à enregistrer sont ou contiennent des identificateurs de données. Si OfficeScan détecte au moins un identificateur de données, aucun fichier ne sera enregistré, pas même ceux qui ne sont pas des identificateurs de données ou qui n'en contiennent pas. OfficeScan peut également empêcher d'éjecter le CD ou le DVD. Dans ce cas, invitez les utilisateurs à redémarrer le processus logiciel ou à réinitialiser l'ordinateur.

OfficeScan applique des règles d'enregistrement sur CD/DVD supplémentaires :

- Pour limiter les faux positifs, OfficeScan ne contrôle pas les fichiers suivants :

```
.bud      .dll      .gif      .gpd      .htm      .ico      .ini

.jpg      .lnk      .sys      .ttf      .url      .xml
```

- Afin d'améliorer les performances, deux types de fichiers utilisés par les enregistreurs de données Roxio (`*.png` et `*.skn`) ne sont pas contrôlés.
- OfficeScan ne contrôle pas les fichiers des répertoires suivants :

```
*:\autoexec.bat                    *:\Windows

..\Application Data                ..\Cookies

..\Local Settings                  ..\ProgramData

..\Program Files                   ..\Users\*\AppData
```

```
..\WINNT
```

- Les images ISO créées par les dispositifs et logiciels ne sont pas contrôlées.

Applications Peer-to-Peer

OfficeScan contrôle les fichiers que les utilisateurs partagent via des applications pair-à-pair.

Pour obtenir la liste des applications Pair à pair prises en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Chiffrement PGP

OfficeScan contrôle les données à encoder par les logiciels de cryptage PGP. OfficeScan vérifie les données avant le chiffremente.

Pour obtenir la liste des logiciels de chiffrement PGP, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Imprimante

OfficeScan contrôle les opérations d'impression lancées depuis diverses applications.

OfficeScan ne bloque pas les opérations d'impression des nouveaux fichiers n'ayant pas été enregistrés, car les informations d'impression n'ont été jusque-là stockées que dans la mémoire.

Pour obtenir la liste des applications pouvant lancer des opérations d'impression prises en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Stockage amovible

OfficeScan contrôle les transmissions de données vers et au sein des périphériques de stockage amovibles. Voici des exemples d'activités liées à la transmission de données :

- Création d'un fichier dans le périphérique

- Copie d'un fichier de l'ordinateur hôte sur le périphérique
- Fermeture d'un fichier modifié dans le périphérique
- Modification des informations de fichier (extension du fichier, par exemple) dans le périphérique

Lorsqu'un fichier à transmettre contient un identificateur de données, OfficeScan bloque ou autorise la transmission.

Remarque

L'action Contrôle des dispositifs est prioritaire par rapport à l'action de la prévention contre la perte de données. Si le contrôle des dispositifs n'autorise pas la copie de fichiers vers un périphérique de stockage, par exemple, la transmission des données sensibles n'aura pas lieu même si la prévention contre la perte de données l'autorise. Pour plus d'informations concernant les actions de contrôle des dispositifs, voir *Autorisations pour les périphériques de stockage à la page 8-3*.

Pour obtenir la liste des périphériques de stockage amovibles et des applications qui facilitent la transmission de données prises en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

La gestion de la transmission de fichiers vers un périphérique de stockage amovible est un processus simple. Par exemple, un utilisateur qui crée un fichier dans Microsoft Word peut souhaiter l'enregistrer sur une carte SD (peu importe le type du fichier à enregistrer). Si le fichier contient un identificateur de données ne devant pas être transmis, OfficeScan empêche l'enregistrement du fichier.

Pour la transmission de fichiers au sein du périphérique, OfficeScan sauvegarde le fichier (si sa taille est inférieure ou égale à 75 Mo) sur `%WINDIR%\system32\dgagent\temp` avant de le traiter. OfficeScan supprime le fichier de sauvegarde s'il a autorisé la transmission du fichier. Si OfficeScan a bloqué la transmission, il est possible que le fichier ait été effacé au cours du processus. Dans ce cas, OfficeScan va copier le fichier de sauvegarde dans le dossier contenant le fichier d'origine.

OfficeScan vous autorise à définir des périphériques non contrôlés. OfficeScan autorise toujours les transmissions de données vers ou au sein de ces périphériques. Identifie les périphériques selon leurs fournisseurs et peut également procurer leurs modèles et numéros de série.

Conseil

À l'aide de l'outil Liste de dispositifs, interrogez les dispositifs reliés aux points finaux. L'outil indique, pour chaque périphérique, le nom du fournisseur, le modèle et le numéro de série. Pour obtenir des informations détaillées, voir *Outil Liste de dispositifs à la page 9-54*.

Logiciel de synchronisation (ActiveSync)

OfficeScan contrôle les données transmises à un dispositif mobile par le biais d'un logiciel de synchronisation.

Pour obtenir la liste des logiciels de synchronisation pris en charge, voir :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Si les données ont une adresse IP source 127.0.0.1 et sont envoyées par les ports 990 ou 5678 (les ports utilisés pour la synchronisation), OfficeScan vérifie si les données sont des identificateurs de données avant d'autoriser ou de bloquer la transmission.

Lorsque OfficeScan bloque un fichier transmis sur le port 990, il se peut qu'un fichier de même nom contenant des caractères malformés soit créé dans le dossier de destination sur le dispositif amovible. Ceci est dû au fait que des parties du fichier ont été copiées sur le dispositif avant que OfficheScan ne bloque la transmission.

Presse-papiers Windows

OfficeScan contrôle les données à transmettre au presse-papiers Windows avant d'autoriser ou de bloquer la transmission.

OfficeScan peut également contrôler les activités du presse-papiers entre l'ordinateur hôte et VMWare ou Remote Desktop. Le contrôle s'effectue sur l'entité avec le client OfficeScan. Un client OfficeScan sur une machine VMWare virtuelle, par exemple, peut empêcher la transmission des données du presse-papiers de la machine virtuelle vers l'ordinateur hôte. De même, un ordinateur hôte avec un client OfficeScan peut ne pas copier les données du presse-papiers sur un point final atteint via Remote Desktop.

Mesures de prévention contre la perte de données

Lorsque OfficeScan détecte la transmission d'identificateurs de données, il vérifie la stratégie DLP pour les identificateurs de données identifiés, puis effectue l'action configurée pour la stratégie.

Le tableau suivant répertorie les actions Prévention contre la perte de données.

TABLEAU 9-5. Mesures de prévention contre la perte de données

ACTION	DESCRIPTION
Actions	
Ignorer	OfficeScan autorise et journalise la transmission
Bloquer	OfficeScan bloque et journalise la transmission
Actions supplémentaires	
Notifier l'utilisateur client	OfficeScan affiche un message de notification pour informer l'utilisateur de la transmission de données et si cette dernière est transmise ou bloquée.
Données d'enregistrement	Indépendamment de l'action principale, OfficeScan enregistre les informations sensibles dans le `<dossier d'installation du client >\DLPLite\Forensic`. Sélectionnez cette action pour évaluer les informations sensibles en cours de marquage par Prévention contre la perte de données. Par mesure de sécurité, les clients n'envoient pas d'informations sensibles enregistrées au serveur. Les informations sensibles enregistrées utilisent trop d'espace disque. De ce fait, Trend Micro recommande fortement de choisir cette option uniquement pour les informations hautement sensibles.

Règles de décompression

Les fichiers contenus dans des fichiers compressés peuvent être scannés pour déceler la présence d'actifs numériques. Pour déterminer les fichiers à scanner, OfficeScan applique les règles suivantes au fichier compressé :

- Taille maximale d'un fichier décompressé : __ Mo (1 à 512 Mo)
- Nombre maximal de couches de compression : __ (1-20)
- Nombre maximal de fichiers à scanner : __ (1-2000)

Règle 1 : Taille maximale d'un fichier décompressé

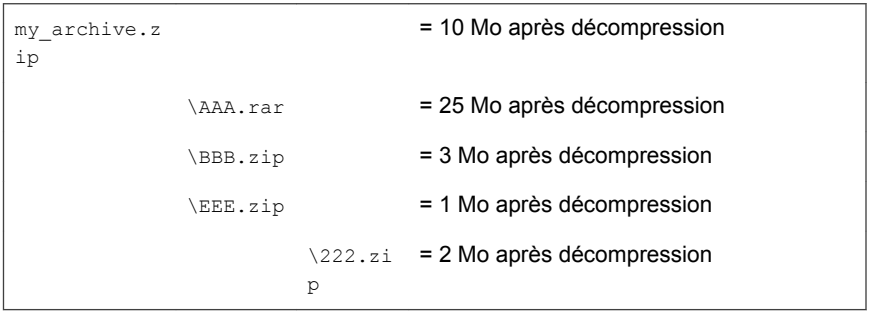
Un fichier compressé, après décompression, ne doit pas dépasser la limite définie.

Exemple : Vous avez défini la limite sur 20 Mo.

Scénario 1 : Si la taille d'un fichier `.zip` après décompression est de 30 Mo, aucun fichier contenu dans le fichier `.zip` ne sera scanné. Les deux autres règles ne sont plus vérifiées.

Scénario 2 : Si la taille du fichier `my_archive.zip` après décompression est de 10 Mo :

- Si `my_archive.zip` ne contient pas de fichiers compressés, OfficeScan ignore la règle 2 et passe à la règle 3.
- Si `my_archive.zip` contient des fichiers compressés, la taille de l'ensemble des fichiers décompressés ne doit pas dépasser la limite. Par exemple, si `my_archive.zip` contient `AAA.rar`, `BBB.zip` et `EEE.zip`, et si `EEE.zip` contient `222.zip` :


my_archive.zip = 10 Mo après décompression
\AAA.rar = 25 Mo après décompression
\BBB.zip = 3 Mo après décompression
\EEE.zip = 1 Mo après décompression
\222.zip = 2 Mo après décompression

`my_archive.zip`, `BBB.zip`, `EEE.zip` et `222.zip` seront vérifiés en fonction de la règle 2 car la taille combinée de ces fichiers ne dépasse pas la limite de 20 Mo. `AAA.rar` est ignoré.

Règle 2 : Nombre maximal de couches de compression

Les fichiers compris dans le nombre de couches spécifiées seront marqués pour le scan.

Par exemple :

```
my_archive.zip
                  \BBB.zip          \CCC.xls
                  \DDD.txt
                  \EEE.zip          \111.pdf
                                    \222.zip          \333.txt
```

Si vous définissez la limite à deux couches :

- OfficeScan ignore le fichier `333.txt` car il se trouve sur la troisième couche.
- OfficeScan indiquera les fichiers suivants pour le scan et vérifiera la règle 3 :
  - `DDD.txt` (sur la première couche)
  - `CCC.xls` (sur la deuxième couche)
  - `111.pdf` (sur la deuxième couche)

Règle 3 : Nombre maximal de fichiers à scanner

OfficeScan effectuera le scan des fichiers jusqu'à la limite indiquée. OfficeScan effectue le scan des fichiers et des dossiers dans l'ordre numérique, puis dans l'ordre alphabétique.

Reprenons l'exemple de la règle 2, OfficeScan a indiqué les fichiers mis en surbrillance pour le scan :

```
my_archive.zip
                  \BBB.zip          \CCC.xls
                  \DDD.txt
                  \EEE.zip          \111.pdf
```

```
                                    \222.zip          \333.txt
```

En outre, `my_archive.zip` contient un dossier nommé `7Folder`, qui n'a pas été vérifié en fonction de la règle 2. Ce dossier contient `FFF.doc` et `GGG.ppt`. Le nombre total de fichiers à scanner est donc de 5, comme indiqué ci-dessous :

```
my_archive.zip
                    \7Folder          \FFF.doc
                    \7Folder          \GGG.ppt
                    \BBB.zip          \CCC.xls
                    \DDD.txt
                    \EEE.zip          \111.pdf
                                      \222.zip          \333.txt
```

Si vous définissez la limite à 4 fichiers, les fichiers suivants seront scannés :

- `FFF.doc`
- `GGG.ppt`
- `CCC.xls`
- `DDD.txt`

Remarque

Pour les fichiers contenant des fichiers imbriqués, OfficeScan extrait le contenu des fichiers imbriqués.

Si le contenu extrait est du texte, le fichier hôte (tel que `123.doc`) et les fichiers imbriqués (tels que `abc.txt` et `xyz.xls`) comptent pour un seul fichier.

Si le contenu extrait n'est pas du texte, le fichier hôte (tel que `123.doc`) et les fichiers imbriqués (tels que `abc.exe`) sont comptés séparément.

Événements qui déclenchent les règles de décompression

Les événements suivants déclenchent les règles de décompression :

- **Événement 1 :**

  Un fichier compressé qui doit être transmis correspond à une stratégie et l'action définie sur le fichier compressé est Ignorer (transmettre le fichier).

  Par exemple, pour contrôler les fichiers .ZIP que les utilisateurs transmettent, vous avez défini un attribut de fichier (.ZIP), l'avez ajouté à un modèle, utilisé ce modèle dans une stratégie et ensuite défini l'action sur **Ignorer**.

  Remarque

  Si l'action définie est Bloquer, le fichier compressé n'est pas transmis et il n'est donc pas nécessaire de scanner les fichiers qu'il contient.

- **Événement 2 :**

  Un fichier compressé à transmettre ne correspond pas à une stratégie.

  Dans ce cas, OfficeScan soumettra le fichier compressé aux règles de décompression afin de déterminer quels fichiers contenus doivent être scannés pour détecter des actifs numériques et s'il faut transmettre ou pas le fichier compressé dans son intégralité.

- **Résultat :**

  Les événements 1 et 2 ont le même résultat. Quand OfficeScan trouve un fichier compressé :

  - Si la règle 1 ne donne pas de résultat, OfficeScan autorise la transmission du fichier compressé dans son intégralité.
  - Si la règle 1 donne un résultat, les deux autres règles sont vérifiées. OfficeScan autorise la transmission du fichier compressé dans son intégralité si :
    - Aucun fichier scanné ne correspond à une stratégie.
    - Tous les fichiers scannés correspondent à une stratégie et l'action définie est **Ignorer**.

      La transmission du fichier compressé dans son intégralité est bloquée si au moins un des fichiers scannés correspond à une stratégie et si l'action définie est **Bloquer**.

Configuration de la stratégie de prévention contre la perte de données

Vous pouvez commencer à créer des stratégies Prévention contre la perte de données une fois que vous avez configuré les identificateurs de données et que vous les avez organisés en modèles.

En plus des identificateurs de données et des modèles, vous devez configurer des canaux et des actions lorsque vous créez une stratégie. Pour plus d'informations sur les stratégies, voir *Stratégies de prévention contre la perte de données à la page 9-11*.

Activation de la prévention contre la perte de données

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Paramètres DLP**.
4. Pour configurer une stratégie applicable aux clients externes, cliquez sur l'onglet **Clients externes** ; pour configurer une stratégie applicable aux clients internes, cliquez sur **Clients internes**.

   Remarque

   Au besoin, configurez les paramètres d'emplacement client. Ces paramètres permettront aux clients de déterminer leur emplacement et d'appliquer la stratégie appropriée Prévention contre la perte de données. Pour obtenir des informations détaillées, voir *Emplacement de l'ordinateur à la page 13-2*.

5. Sélectionnez **Activer la prévention contre la perte de données**.
6. Choisissez l'un des éléments suivants :

   - Si vous êtes sur l'onglet **Clients externes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients internes**.

- Si vous êtes sur l'onglet **Clients internes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients externes**.

7. Configurez les paramètres suivants :

   - *Configuration des paramètres des modèles à la page 9-51*
   - *Configuration des paramètres des canaux à la page 9-52*
   - *Configuration des paramètres des actions à la page 9-54*

8. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Configuration des paramètres des modèles

Tâche

1. Cliquez sur l'onglet **Modèle**.
2. Choisissez l'un des éléments suivants :

   - Si vous êtes sur l'onglet **Clients externes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients internes**.
   - Si vous êtes sur l'onglet **Clients internes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients externes**.

3. Dans la liste **Modèles disponibles**, sélectionnez des modèles, puis cliquez sur **Ajouter**. Lorsque vous sélectionnez des modèles :

   - Sélectionnez des entrées multiples en appuyant et en maintenant la touche **CTRL** enfoncée, puis sélectionnez les modèles.
   - Si vous recherchez un modèle spécifique, utilisez la fonction de recherche. Vous pouvez y saisir tout ou partie du nom du modèle.

4. Si votre modèle favori ne se trouve pas dans la liste des **Modèles disponibles** :

   a. cliquez sur **Ajouter un nouveau modèle**. L'écran Modèles de prévention contre la perte de données s'affiche. Pour obtenir des instructions sur l'ajout de modèles dans l'écran Modèles de prévention des données, voir *Modèles de prévention contre la perte de données à la page 9-27*.

   b. Une fois le modèle créé, sélectionnez-le et cliquez sur **Ajouter**.

Remarque

OfficeScan utilise la règle de première correspondance lors de la vérification des modèles. Cela signifie que si un fichier ou des données correspondent à la définition contenue dans un modèle, OfficeScan arrête ses recherches. La priorité se base sur l'ordre des modèles dans la liste.

Configuration des paramètres des canaux

Tâche

1. Cliquez sur l'onglet **Canal**.
2. Choisissez l'un des éléments suivants :

   - Si vous êtes sur l'onglet **Clients externes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients internes**.
   - Si vous êtes sur l'onglet **Clients internes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients externes**.

3. Sélectionnez les canaux pour la stratégie. Pour plus d'informations sur les canaux, voir *Canaux réseau à la page 9-32* et *Canaux système et application à la page 9-40*.

4. Si vous avez sélectionné l'un des canaux réseau :

   a. Sélectionnez l'étendue de transmission.

      - **Toutes les transmissions**
      - **Uniquement les transmissions hors du réseau local**

   b. Cliquez sur **Exceptions**.

   c. Indiquez les cibles contrôlées et non contrôlées.

   Pour plus d'informations sur l'étendue de transmission, l'influence de l'étendue de transmission sur les cibles et la manière de définir des cibles correctement, voir *Étendue et cibles de transmission pour les canaux réseau à la page 9-37*.

5. Si vous avez sélectionné **Clients de messagerie** :

   a. Cliquez sur **Exceptions**.

   b. Indiquez les domaines de messagerie internes contrôlés et non contrôlés. Pour plus d'informations sur les domaines de messagerie contrôlés et non contrôlés, voir *Clients de messagerie à la page 9-33*.

6. Si vous avez sélectionné **Stockage amovible** :

   a. Cliquez sur **Exceptions**.

   b. Ajoutez des périphériques de stockage amovibles non contrôlés en les identifiant par leurs fournisseurs. Le modèle et le numéro de série du périphérique sont facultatifs.

   c. Pour ajouter plusieurs périphériques, cliquez sur l'icône **+**.

Conseil

À l'aide de l'outil Liste de dispositifs, interrogez les dispositifs reliés aux points finaux. L'outil indique, pour chaque périphérique, le nom du fournisseur, le modèle et le numéro de série. Pour obtenir des informations détaillées, voir *Outil Liste de dispositifs à la page 9-54*.

Configuration des paramètres des actions

Tâche

1. Cliquez sur l'onglet **Action**.
2. Choisissez l'un des éléments suivants :
   - Si vous êtes sur l'onglet **Clients externes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients internes**.
   - Si vous êtes sur l'onglet **Clients internes**, vous pouvez appliquer tous les paramètres Prévention contre la perte de données pour les clients internes en sélectionnant **Appliquer tous les paramètres aux clients externes**.
3. Sélectionnez une action principale et toute action complémentaire applicable. Pour plus d'informations sur les actions, voir *Mesures de prévention contre la perte de données à la page 9-45*.
4. Configurez les paramètres pour les règles de décompression. Pour plus d'informations sur les règles de décompression, voir *Règles de décompression à la page 9-45*.

Outil Liste de dispositifs

Exécutez localement l'outil Liste de dispositifs sur chaque point final pour interroger les dispositifs externes qui y sont connectés. L'outil scanne un point final à la recherche de dispositifs externes, puis affiche les informations relatives à ce dispositif dans une fenêtre de navigateur. Vous pouvez ensuite utiliser les informations lors de la

configuration des paramètres des dispositifs pour la prévention contre la perte de données et le contrôle des dispositifs.

Exécution de l'outil Liste de dispositifs

Tâche

1. Sur l'ordinateur serveur OfficeScan, accédez à `\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Copiez `listDeviceInfo.exe` sur le point final cible.
3. Sur le point final, double-cliquez sur `listDeviceInfo.exe`.
4. Les informations relatives au dispositif s'affichent dans la fenêtre de navigation qui s'ouvre. La prévention contre la perte de données et le contrôle des dispositifs utilisent les informations suivantes :
   - Revendeur (obligatoire)
   - Modèle (facultatif)
   - ID de série (facultatif)

Notifications de la prévention contre la perte de données

OfficeScan est fourni avec un ensemble de messages de notification par défaut informant les administrateurs et les utilisateurs clients OfficeScan des transmissions d'actifs numériques.

Pour plus de détails sur les notifications envoyées aux administrateurs, voir *Notifications de la prévention contre la perte de données pour les administrateurs à la page 9-56*.

Pour plus de détails sur les notifications envoyées aux utilisateurs clients, voir *Notifications de prévention contre la perte de données pour les utilisateurs clients à la page 9-59*.

Notifications de la prévention contre la perte de données pour les administrateurs

Configurez OfficeScan afin d'envoyer aux administrateurs une notification lorsqu'il détecte la transmission d'actifs numériques, ou uniquement lorsque la transmission est bloquée.

OfficeScan est fourni avec un ensemble de messages de notification par défaut informant les administrateurs des transmissions d'actifs numériques. Modifiez les notifications et configurez les paramètres de notification supplémentaires pour répondre aux exigences de l'entreprise.

Remarque

OfficeScan peut vous envoyer des notifications par courrier électronique, pageur, déroutement SNMP et par le journal des événements de Windows NT. Configurez les paramètres lorsqu'OfficeScan envoie des notifications par le biais de ces chaînes. Pour obtenir des informations détaillées, voir .

Configuration de la notification de prévention contre la perte de données pour les administrateurs

Tâche

1. Accédez à **Notifications** > **Notifications administrateur** > **Notifications standard**.
2. Sous **Critères** l'onglet :
   a. Accédez à la section **Transmissions des actifs numériques**.
   b. Spécifiez si l'envoi des notifications doit être effectué lorsque la transmission d'actifs numériques est détectée (l'action peut être bloquée ou omise) ou uniquement lorsque la transmission est bloquée.
3. Sous **E-mail** l'onglet :
   a. Accédez à la section **Transmissions des actifs numériques**.
   b. Sélectionnez **Activer la notification par courrier électronique**.

c. Sélectionnez **Envoyer les notifications aux utilisateurs ayant les droits d'accès au domaine de l'arborescence des clients**.

Utilisez Role-based Administration afin d'accorder aux utilisateurs l'accès au domaine de l'arborescence des clients. Si une transmission se produit sur un client appartenant à un domaine spécifique, le courrier électronique est envoyé aux adresses électroniques des utilisateurs ayant les autorisations sur ce domaine. Pour des exemples, voir le tableau suivant :

TABLEAU 9-6. Domaines et droits d'accès de l'arborescence des clients

DOMAINE DE L'ARBORESCENCE DES CLIENTS	RÔLES AVEC DROITS D'ACCÈS AU DOMAINE	COMPTE UTILISATEUR AVEC LE RÔLE	ADRESSE ÉLECTRONIQUE POUR LE COMPTE UTILISATEUR
Domaine A	Administrateur (intégré)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domaine B	Administrateur (intégré)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un client OfficeScan appartenant au domaine A détecte une transmission d'actifs numériques, le courrier électronique sera envoyé à mary@xyz.com, john@xyz.com, et chris@xyz.com.

Si un client appartenant au domaine B détecte la transmission, le courrier électronique est envoyé à mary@xyz.com et jane@xyz.com.

Remarque

Si vous activez cette option, tous les utilisateurs disposant des autorisations sur ce domaine doivent avoir une adresse électronique correspondante. La notification par courrier électronique ne sera pas envoyée aux utilisateurs qui n'ont pas d'adresse électronique. Les utilisateurs et les adresses électroniques sont configurés à partir de **Administration** > **Comptes utilisateurs**.

d. Sélectionnez **Envoyer les notifications à/aux (l')adresse(s) électronique(s) suivante(s)**, puis saisissez les adresses électroniques.

e. Acceptez ou modifiez l'objet et le message par défaut. Utilisez des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 9-7. Variables de jeton pour les notifications de prévention contre la perte de données

VARIABLE	DESCRIPTION
%USER%	L'utilisateur s'est connecté à l'ordinateur lorsque une transmission a été détectée
%COMPUTER%	Ordinateur sur lequel la transmission a été détectée
%DOMAIN%	Domaine de l'ordinateur
%DATETIME%	Date et heure auxquelles la transmission a été détectée
%CHANNEL%	Le canal par lequel la transmission a été détectée
%TEMPLATE%	Le modèle d'actifs numériques ayant déclenché la détection

4. Sous l'onglet **Pageur** :

   a. Accédez à la section **Transmissions des actifs numériques**.

   b. Sélectionnez **Activer la notification par pageur**.

   c. Saisissez le message.

5. Sous l'onglet **Déroutement SNMP** :

   a. Accédez à la section **Transmissions des actifs numériques**.

   b. Sélectionnez **Activer la notification par déroutement SNMP**.

   c. Acceptez ou modifiez le message par défaut. Utilisez des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 9-7 à la page 9-58* pour obtenir des informations détaillées.

6. Sous l'onglet **Journal d'événements NT** :

   a. Accédez à la section **Transmissions des actifs numériques**.

b. Sélectionnez **Activer la notification via le journal d'événements NT**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 9-7 à la page 9-58* pour obtenir des informations détaillées.

7. Cliquez sur **Enregistrer**.

Notifications de prévention contre la perte de données pour les utilisateurs clients

OfficeScan peut afficher des messages de notification sur les ordinateurs clients immédiatement après avoir accepté ou bloqué la transmission d'actifs numériques.

Pour avertir les utilisateurs que la transmission des actifs numériques a été bloquée ou acceptée, sélectionnez l'option **Notifier l'utilisateur client** lors de la création d'une stratégie Prévention contre la perte de données. Pour obtenir des instructions sur la création d'une stratégie, voir *Configuration de la stratégie de prévention contre la perte de données à la page 9-50*.

Configuration de la notification de prévention contre la perte de données pour les clients

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.
2. Cliquez sur l'onglet **Transmissions des actifs numériques**.
3. Acceptez ou modifiez le message par défaut.
4. Cliquez sur **Enregistrer**.

Journaux de prévention contre la perte de données

Les clients consignent les transmissions d'actifs numériques (transmissions bloquées et autorisées) et envoient immédiatement les journaux au serveur. Si le client ne parvient pas à envoyer des journaux, un deuxième essai a lieu au bout de 5 minutes.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de prévention contre la perte de données

Tâche

1. Accédez à **Notifications** > **Notifications administrateur** > **Notifications standard**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Journaux** > **Journaux de prévention contre la perte de données** ou **Afficher journaux** > **Journaux de prévention contre la perte de données**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date/heure à laquelle la transmission d'actif numérique a été détectée
   - Ordinateur sur lequel la transmission a été détectée
   - Domaine de l'ordinateur
   - Adresse IP de l'ordinateur

- Processus qui a facilité la transmission d'un actif numérique. Le processus dépend du canal. Pour obtenir des informations détaillées, voir *Processus par canal à la page 9-61*.
- Canal par l'intermédiaire duquel l'actif numérique a été transmis
- Action sur la transmission
- Modèle qui a déclenché la détection
- Nom de l'utilisateur connecté à l'ordinateur
- Destination vers laquelle l'actif numérique a été transmis
- Description, qui comporte des informations complémentaires sur la transmission. Pour obtenir des informations détaillées, voir *Descriptions à la page 9-64*.

6. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Processus par canal

Le tableau suivant établit une liste des processus qui s'affichent sous la colonne Processus des journaux Prévention contre la perte de données.

TABLEAU 9-8. Processus par canal

CANAL	PROCESSUS
Logiciel de synchronisation (ActiveSync)	Chemin d'accès complet et nom de processus du logiciel de synchronisation Exemple : `C:\Windows\system32\WUDFHost.exe`
Enregistreur de données (CD/DVD)	Chemin complet et nom de processus de l'enregistreur de données Exemple : `C:\Windows\Explorer.exe`

CANAL	PROCESSUS
Presse-papiers Windows	Chemin complet et nom de processus de ShowMsg.exe `ShowMsg.exe` est le processus Prévention contre la perte de données qui contrôle les événements du presse-papiers. Exemple : `C:\Windows\system32\ShowMsg.exe`
Client de messagerie - Lotus Notes	Chemin complet et nom de processus de Lotus Notes Exemple : `C:\Program Files\IBM\Lotus\Notes\nlnotes.exe`
Client de messagerie - Microsoft Outlook	Chemin complet et nom de processus de Microsoft Outlook Exemple : `C:\Program Files\Microsoft Office\Office12\ OUTLOOK.EXE`
Client de messagerie - Tous les clients qui utilisent le protocole SMTP	Chemin complet et nom de processus du client de messagerie Exemple : `C:\Program Files\Mozilla Thunderbird\thunderbird.exe`
Stockage amovible	Nom de processus de l'application qui a transmis les données vers le périphérique de stockage ou au sein de celui-ci Exemple : `explorer.exe`
FTP	Chemin complet et nom de processus du client FTP Exemple : `D:\Program Files\FileZilla FTP Client\filezilla.exe`
HTTP	«Application HTTP»

CANAL	PROCESSUS
HTTPS	Chemin complet et nom de processus du navigateur ou de l'application Exemple : `C:\Program Files\Internet Explorer\iexplore.exe`
Application de messagerie instantanée	Chemin complet et nom de processus de l'application de messagerie instantanée Exemple : `C:\Program Files\Skype\Phone\Skype.exe`
Application de messagerie instantanée - MSN	• Chemin complet et nom de processus de MSN Exemple : `C:\Program Files\Windows Live\Messenger\ msnmsgr.exe` • «Application HTTP» si les données sont transmises à partir d'une fenêtre de conversation
Application Pair à pair	Chemin complet et nom de processus de l'application Pair à pair Exemple : `D:\Program Files\BitTorrent\bittorrent.exe`
Chiffrement PGP	Chemin complet et nom de processus du logiciel de chiffrement PGP Exemple : `C:\Program Files\PGP Corporation\PGP Desktop\ PGPmnApp.exe`
Imprimante	Chemin complet et nom de processus de l'application qui a initié une opération d'impression Exemple : `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`

CANAL	PROCESSUS
Protocole SMB	Chemin complet et nom de processus de l'application à partir de laquelle l'accès aux fichiers partagés (copie ou création d'un nouveau fichier) a été effectué Exemple : `C:\Windows\Explorer.exe`
Webmail (mode HTTP)	«Application HTTP»
Webmail (mode HTTPS)	Chemin complet et nom de processus du navigateur ou de l'application Exemple : `C:\Program Files\Mozilla Firefox\firefox.exe`

Descriptions

La colonne **Description** des journaux Prévention contre la perte de données affiche des informations supplémentaires sur la transmission d'actifs numériques. Les informations sont séparées par des virgules et ne sont disponibles que si la transmission s'effectue à travers certains canaux. Une description contenant plus de 256 caractères est automatiquement tronquée.

Le tableau suivant établit une liste des informations s'affichant.

TABLEAU 9-9. Descriptions de la transmission des actifs numériques

CANAL	DÉTAILS
Client de messagerie - Lotus Notes	• Adresses e-mail des destinataires dans les champs À/Cc/Cci Les adresses e-mail sont au format X.400 ou SMTP. • Adresse e-mail de l'expéditeur
Client de messagerie - Microsoft Outlook	• Adresses e-mail des destinataires dans les champs À/Cc/Cci Les adresses e-mail sont au format X.400 ou SMTP. • Nom de l'expéditeur

CANAL	DÉTAILS
Client de messagerie - Tous les clients qui utilisent le protocole SMTP	• Adresses e-mail des destinataires dans les champs À/Cc/Cci • Adresse e-mail de l'expéditeur • Objet du courrier électronique
FTP	Nom d'utilisateur utilisé pour la connexion au serveur FTP
HTTP/HTTPS	URL d'un site Web ou d'une page Web
Webmail	• URL Webmail • Adresses e-mail des destinataires dans les champs À/Cc/Cci • Adresse e-mail de l'expéditeur

Journaux de débogage de protection des données

Activation de la journalisation de débogage pour le module Protection des données

Tâche

1. Obtenez le fichier `logger.cfg` auprès de votre service d'assistance.
2. Ajoutez les données suivantes dans `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
   - **Type** : `chaîne`
   - **Nom**: `debugcfg`
   - **Valeur** : `C:\Log\logger.cfg`
3. Créez un dossier intitulé « Log » dans le `C:\ directory`.
4. Copiez le fichier `logger.cfg` dans le dossier « Log ».
5. Déployez la prévention contre la perte des données et les paramètres de contrôle des dispositifs depuis la console Web pour lancer la collecte de journaux.

Remarque

Désactivez la journalisation de débogage pour le module Protection des données en supprimant `debugcfg` dans la clé de registre et en redémarrant l'ordinateur.

Désinstallation de la protection des données

Si vous désinstallez le module Protection des données à partir de Plug-In Manager :

- Toutes les configurations de prévention contre la perte de données, les paramètres et les journaux sont supprimés du serveur OfficeScan.
- Tous les paramètres et configurations du contrôle des dispositifs fournis par le module de protection des données sont supprimés du serveur.
- Le module de protection des données est supprimé des clients. Il faut redémarrer les ordinateurs clients pour supprimer complètement la protection des données.
- Les stratégies de prévention contre la perte de données ne seront plus appliquées sur les clients.
- Le contrôle des dispositifs ne surveille plus l'accès aux dispositifs suivants :
  - Ports COM et LPT
  - Interface IEEE 1394
  - Périphériques d'images
  - Périphériques infrarouges
  - Modems
  - Carte PCMCIA
  - Touche Impr. écran

Réinstallez le module Protection des données à tout moment. Après la réinstallation, activez la licence en utilisant un code d'activation valide.

Désinstallez la protection de données à partir de Plug-In Manager

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Dans l'écran **Plug-in Manager**, accédez à la section **Protection des données OfficeScan** et cliquez sur **Désinstaller**.
3. Surveillez la progression de la désinstallation. Vous pouvez naviguer dans une autre fenêtre pendant l'opération.
4. Actualisez l'écran **Plug-in Manager** après la désinstallation. OfficeScan La protection des données est à nouveau disponible pour l'installation.

Chapitre 10

Protection des ordinateurs contre les menaces Internet

Ce chapitre décrit les menaces provenant d'Internet et l'utilisation de OfficeScan pour protéger votre réseau et vos ordinateurs des menaces provenant d'Internet.

Sujets abordés dans ce chapitre :

- *À propos des menaces Internet à la page 10-2*
- *Réputation de sites Web à la page 10-2*
- *Stratégies de réputation de sites Web à la page 10-3*
- *Proxy pour l'évaluation de la réputation de sites Web à la page 10-9*
- *Notifications sur les menaces Internet pour les utilisateurs clients à la page 10-10*
- *Journaux de réputation de sites Web à la page 10-11*

À propos des menaces Internet

Les menaces Internet comprennent un large éventail de menaces provenant du Web. Les menaces Internet emploient des méthodes très sophistiquées : au lieu d'utiliser une seule approche ou un seul fichier, elles associent plusieurs techniques et fichiers. Par exemple, les auteurs de menaces Internet modifient constamment la version ou la variante utilisée. Étant donné qu'une menace Internet se trouve à un emplacement défini sur un site Web plutôt que sur un ordinateur infecté, l'auteur de cette menace Internet modifie constamment son code pour éviter qu'elle ne soit détectée.

Au cours de ces dernières années, les individus que l'on qualifiait auparavant de pirates, auteurs de virus, spammeurs et créateurs de spywares sont désormais connus sous le nom de cybercriminels. Ces individus utilisent les menaces Internet pour poursuivre deux objectifs. Le premier est de dérober des informations pour les revendre ensuite. Il en résulte une divulgation d'informations confidentielles et une perte d'identité. L'ordinateur infecté peut également devenir un vecteur pour transmettre des attaques de phishing ou d'autres activités d'interception d'informations. Entre autres, cette menace risque d'entamer la confiance dans le commerce en ligne et l'économie numérique. Le second objectif est de pirater la puissance de l'UC d'un utilisateur et de l'utiliser comme instrument pour mener des activités lucratives. Ces activités incluent l'envoi de spam ou l'escroquerie sous la forme d'attaques distribuées de refus de service ou d'activités facturées au clic.

Réputation de sites Web

La technologie de réputation de sites Web assure le suivi de la crédibilité des domaines Web en leur attribuant un score de réputation, basé sur des facteurs tels que l'ancienneté du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. Elle continue ensuite à analyser les sites et à bloquer les utilisateurs tentant d'accéder à ceux qui sont infectés.

Les clients OfficeScan envoient des requêtes aux sources Smart Protection pour déterminer la réputation des sites Web auxquels les utilisateurs tentent d'accéder. La réputation d'un site Web est liée à la stratégie de réputation de sites Web qui est appliquée sur l'ordinateur. Selon la stratégie utilisée, le client OfficeScan bloquera ou autorisera l'accès au site Web.

Remarque

Pour plus d'informations concernant les sources Smart Protection, voir *Liste des sources Smart Protection à la page 3-23*.

Ajoutez les sites Web que vous considérez sûrs dans la liste des sites approuvés, et ceux que vous considérez dangereux dans la liste des sites bloqués. Lorsqu'un client OfficeScan détecte l'accès à l'un de ces sites Web, il autorise ou bloque automatiquement l'accès et cesse d'envoyer des requêtes aux sources Smart Protection.

Stratégies de réputation de sites Web

Les stratégies de réputation de sites Web indiquent à OfficeScan de bloquer ou d'autoriser l'accès à un site Web donné.

Vous pouvez configurer les stratégies pour les clients internes et externes. Les administrateurs OfficeScan configurent généralement une stratégie plus stricte pour les clients externes.

Les stratégies sont des paramètres détaillés dans l'arborescence des clients OfficeScan. Vous pouvez appliquer des stratégies spécifiques à des groupes de clients ou à des clients individuels. Vous pouvez également appliquer une stratégie unique à tous les clients.

Une fois que vous avez déployé les stratégies, les clients utilisent les critères d'emplacement définis dans l'écran Emplacement de l'ordinateur (voir *Emplacement de l'ordinateur à la page 13-2*) afin de déterminer leur emplacement et la stratégie à appliquer. Les clients changent de stratégie à chaque fois que l'emplacement change.

Configuration de Stratégie de réputation de sites Web

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Sélectionnez les cibles dans l'arborescence client.

- Pour configurer une stratégie pour les clients fonctionnant sous Windows XP, Vista, ou 7, sélectionnez l'icône du domaine racine ( ), des domaines spécifiques ou des clients.

  Remarque

  Après avoir sélectionné le domaine racine ou des domaines spécifiques, le paramètre ne s'appliquera qu'aux clients exécutant Windows XP, Vista ou 7. Le paramètre ne s'appliquera pas aux clients exécutant Windows Server 2003 ou Windows Server 2008, même s'ils font partie des domaines.

- Pour configurer une stratégie pour les clients fonctionnant sous Windows Server 2003 ou Windows Server 2008, sélectionnez un client spécifique.

3. Cliquez sur **Paramètres** > **Paramètres de réputation de sites Web**.

4. Pour configurer une stratégie applicable aux clients externes, cliquez sur l'onglet **Clients externes** ; pour configurer une stratégie applicable aux clients internes, cliquez sur **Clients internes**.

   Conseil

   Au besoin, configurez les paramètres d'emplacement client. Ces paramètres permettront aux clients de déterminer leur emplacement et d'appliquer la stratégie de contrôle de réputation de sites Web appropriée. Pour obtenir des informations détaillées, voir *Emplacement de l'ordinateur à la page 13-2*.

5. Sélectionnez **Activer la stratégie de réputation de sites Web sur les systèmes d'exploitation suivants**. Les systèmes d'exploitation répertoriés dans la fenêtre dépendent des cibles que vous avez sélectionnées à l'étape 1.

   Conseil

   Trend Micro recommande de désactiver la stratégie de réputation de sites Web pour les clients internes si vous utilisez déjà un produit Trend Micro doté de la fonction de réputation de sites Web, tel qu'InterScan Web Security Virtual Appliance.

Lorsqu'une stratégie de réputation de sites Web est activée :

- Les clients externes envoient des requêtes de réputation de sites Web à Smart Protection Network.
- Les clients internes envoient des requêtes de réputation de sites Web :
  - aux serveurs Smart Protection Server si l'option **Envoyer des requêtes aux serveurs Smart Protection Server** est activée. Pour plus d'informations sur cette option, voir l'étape 7.
  - à Smart Protection Network si l'option **Envoyer des requêtes aux serveurs Smart Protection Server** est désactivée.

6. Sélectionnez **Activer l'évaluation**.

Remarque

En mode d'évaluation, les clients autorisent l'accès à tous les sites Web mais enregistrent les accès aux sites qui sont censés être bloqués lorsque l'évaluation est désactivée. Le mode d'évaluation de Trend Micro a été conçu pour vous permettre d'évaluer les sites Web et prendre les mesures qui vous semblent appropriées. Par exemple, les sites Web que vous considérez sûrs peuvent être ajoutés à la liste des URL approuvées.

7. Sélectionnez **Vérifier les URL HTTPS**.

   La communication HTTPS utilise des certificats pour identifier les serveurs Web. Les données sont chiffrées pour éviter le vol et l'espionnage. Bien que l'accès à ces URL soit plus sécurisé, accéder à des sites Web HTTPS comporte toujours des risques. Les sites compromis, même ceux qui possèdent un certificat valide, peuvent contenir des programmes malveillants et dérober des informations personnelles. En outre, les certificats sont assez simples à obtenir, ce qui facilite l'installation de serveurs Web malveillants utilisant HTTPS.

   Activez la vérification des URL HTTPS afin de réduire les risques d'exposition aux sites compromis et malveillants qui utilisent HTTPS. OfficeScan peut surveiller le trafic HTTPS dans les navigateurs suivants :

TABLEAU 10-1. Navigateurs pris en charge pour le trafic HTTPS

PARCOURIR	VERSION
Microsoft Internet Explorer	• 6 avec SP2 ou supérieure • 7.x • 8.x • 9.x
Mozilla Firefox	de 3.5 à 11.0

8. Sélectionnez **Ne scanner que les ports HTTP courants** pour restreindre le scan de réputation des sites Web au trafic à travers les ports 80, 81, et 8080. Par défaut, OfficeScan scanne tout le trafic au travers de tous les ports.

9. Sélectionnez **Envoyer des requêtes aux serveurs Smart Protection Server** pour que les clients internes envoient des requêtes de réputation de sites Web aux serveurs Smart Protection Server.

   - Si vous activez cette option :

     - Les clients consultent la liste des sources Smart Protection pour savoir à quels serveurs Smart Protection Server envoyer les requêtes. Pour plus d'informations sur la liste des sources Smart Protection, voir *Liste des sources Smart Protection à la page 3-23*..

     - Assurez-vous que les serveurs Smart Protection Server sont disponibles. Si aucun serveur Smart Protection Server n'est disponible, les clients n'envoient pas de requêtes à Smart Protection Network. Les seules sources restantes de données de réputation de sites Web pour les clients sont les listes des URL approuvées et bloquées (configurées à l'étape 10).

     - Si vous souhaitez que les clients se connectent Serveurs Smart Protection Server via un serveur proxy, spécifiez les paramètres proxy dans l'onglet **Administration** > **Paramètres proxy > Proxy interne**.

     - Assurez-vous de mettre régulièrement à jour Serveurs Smart Protection Server de sorte que la protection reste efficace.

- Les clients ne bloqueront pas les sites Web qui n'ont pas été testés. Les serveurs Smart Protection Server ne stockent pas les données de réputation de sites Web pour ces sites.

- Si vous désactivez cette option :
  - Les clients envoient des requêtes de réputation de sites Web vers Smart Protection Network. Les ordinateurs clients doivent disposer d'une connexion Internet pour pouvoir envoyer les requêtes.
  - Si la connexion à Smart Protection Network nécessite l'authentification du serveur proxy, indiquez les informations d'authentification dans **Administration** > **Paramètres proxy > Proxy externe (onglet)** > **Connexion du client aux serveurs Trend Micro**.
  - Les clients bloqueront les sites Web non testés si vous sélectionnez **Bloque les pages qui n'ont pas été testées par Trend Micro** à l'étape 9.

10. Sélectionnez l'un des niveaux de sécurité de la fonction de réputation de sites Web : **Élevé**, **Moyen** ou **Faible**

Remarque

Les niveaux de sécurité déterminent si OfficeScan autorise ou bloque l'accès à un URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, OfficeScan ne bloque que les URL qui constituent des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de faux positifs augmente également.

11. Si vous désactivez l'option **Veuillez envoyer vos questions aux serveurs Smart Protection Server** dans l'étape 7, vous pouvez sélectionner **Bloque les pages qui n'ont pas été testées par Trend Micro**.

Remarque

Bien que Trend Micro teste activement la sécurité des pages Web, les utilisateurs peuvent rencontrer des pages non testées lorsqu'ils visitent des sites Web nouveaux ou peu consultés. Le blocage de l'accès aux pages non testées peut améliorer la sécurité, mais il peut également empêcher l'accès à des pages sûres.

12. Configurez les listes d'approbation et de blocage.

> **Remarque**
>
> La liste approuvée est prioritaire sur la liste bloquée. Lorsqu'une URL correspond à une entrée de la liste des URL approuvées, les clients autorisent toujours l'accès à cette URL, même si elle figure dans la liste des URL bloquées.

a. Sélectionnez **Activer la liste des URL approuvées/bloquées**.

b. Entrez une URL.

Vous pouvez ajouter un caractère générique (*) à tout emplacement dans l'URL.

Par exemple :

- Si vous entrez `www.trendmicro.com/*`, cela signifie que toutes les pages du site Web Trend Micro seront approuvées.
- Si vous entrez `*.trendmicro.com/*`, cela signifie que toutes les pages appartenant à un sous-domaine de trendmicro.com seront approuvées.

Vous pouvez également entrer des URL contenant des adresses IP. Si une URL contient une adresse IPv6, précisez l'adresse entre parenthèses.

c. Cliquez sur **Ajouter à la liste des URL approuvées** ou **Ajouter à la liste des URL bloquées**.

d. Pour exporter la liste dans un fichier `.dat`, cliquez sur **Exporter**, puis sur **Enregistrer**.

e. Si vous avez exporté une liste à partir d'un autre serveur et souhaitez l'importer dans cet écran, cliquez sur **Importer** et localisez le fichier `.dat`. La liste est chargée à l'écran.

13. Pour soumettre des commentaires relatifs à l'évaluation de réputation de sites Web, cliquez sur **Réévaluer l'URL**. Le système de requête du service d'évaluation de la réputation de sites Web de Trend Micro s'ouvre dans une fenêtre de navigateur.

14. Choisissez d'autoriser ou non l'envoi par le client OfficeScan de journaux de réputation de sites Web au serveur. Autorisez les clients à envoyer des journaux si

vous souhaitez analyser les URL bloqués par OfficeScan puis entreprenez l'action appropriée sur les URL dont vous estimez l'accès sécurisé.

15. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Proxy pour l'évaluation de la réputation de sites Web

Spécifiez les informations d'authentification du serveur proxy si vous avez défini un serveur proxy pour gérer la communication HTTP dans votre entreprise et si une authentification est requise avant que l'accès au Web ne soit autorisé. OfficeScan utilise ces informations d'authentification lors de la connexion aux sources Smart Protection pour déterminer si les sites Web auxquels les utilisateurs tentent d'accéder sont sûrs.

Cette version d'OfficeScan ne prend en charge qu'un ensemble d'informations d'authentification.

Pour plus de détails sur la configuration des paramètres de proxy, reportez-vous à *Proxy externe pour les clients OfficeScan à la page 13-51*.

Notifications sur les menaces Internet pour les utilisateurs clients

OfficeScan peut afficher un message de notification sur un ordinateur client OfficeScan immédiatement après avoir bloqué une URL qui viole une stratégie de réputation de sites Web. Il vous faut activer le message de notification et, de façon facultative, modifier son contenu.

Activation des messages de notification sur les menaces Internet

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres de réputation de sites Web**.
5. Sélectionnez **Afficher une notification lorsqu'un site Web est bloqué**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Modification des messages de notification sur les menaces Internet

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.
2. Cliquez sur l'onglet **Violations de la réputation de sites Web**.
3. Saisissez le message par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de réputation de sites Web

Configurez les clients internes et externes de façon à ce qu'ils envoient des journaux de réputation de sites Web au serveur. Effectuez cette action si vous souhaitez analyser les URL bloqués par OfficeScan et entreprendre les actions appropriées à l'encontre des URL auxquels vous estimez pouvoir accéder en toute sécurité.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage de journaux de réputation de sites Web

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité** ou à **Ordinateurs en réseau** > **Gestion des clients**.

2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Afficher journaux** > **Journaux de réputation de sites Web** ou **Journaux** > **Journaux de réputation de sites Web**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date/heure à laquelle OfficeScan a bloqué l'URL
   - Ordinateur depuis lequel l'utilisateur a accédé à l'URL
   - Domaine de l'ordinateur depuis lequel l'utilisateur a accédé à l'URL
   - URL bloqué
   - Niveau de risque de l'URL
   - Lien vers le système de requête de l'évaluation de la réputation de sites Web de Trend Micro qui fournit de plus amples informations sur l'URL bloqué
6. S'il existe des URL qui ne doivent pas être bloquées, cliquez sur le bouton **Ajouter à la liste des sites approuvés** pour ajouter le site Web à la liste des URL approuvées/bloquées.
7. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Chapitre 11

Utilisation du pare-feu OfficeScan

Ce chapitre décrit les fonctionnalités et les configurations du pare-feu OfficeScan.

Sujets abordés dans ce chapitre :

- *À propos du pare-feu OfficeScan à la page 11-2*
- *Activation ou désactivation du pare-feu OfficeScan à la page 11-6*
- *Stratégies et profils de pare-feu à la page 11-8*
- *Privilèges du pare-feu à la page 11-24*
- *Paramètres généraux du pare-feu à la page 11-27*
- *Notifications de violation du pare-feu pour les utilisateurs clients OfficeScan à la page 11-28*
- *Journaux de pare-feu à la page 11-30*
- *Épidémies de violation du pare-feu à la page 11-32*
- *Test du pare-feu OfficeScan à la page 11-34*

À propos du pare-feu OfficeScan

Le pare-feu OfficeScan protège les clients et les serveurs du réseau grâce à une fonction Stateful inspection et à des scans antivirus de réseau haute performance. Via la console d'administration centralisée, vous pouvez créer des règles pour filtrer les connexions par application, adresse IP, numéro de port ou protocole, puis appliquer les règles à différents groupes d'utilisateurs.

Remarque

vous pouvez activer, configurer et utiliser le pare-feu OfficeScan sur les ordinateurs Windows XP dont le pare-feu Windows est également activé. Cependant, vous devez gérer attentivement vos stratégies pour éviter de créer des stratégies de pare-feu conflictuelles et de produire des résultats inattendus. Consultez la documentation Microsoft pour obtenir des informations détaillées sur le pare-feu Windows.

Le pare-feu OfficeScan inclut les fonctionnalités et améliorations clés suivantes :

- *Filtrage du trafic à la page 11-2*
- *Filtrage d'applications à la page 11-3*
- *Liste Certified Safe Software à la page 11-3*
- *Recherche de virus de réseau à la page 11-3*
- *Profils et stratégies personnalisables à la page 11-4*
- *Stateful Inspection à la page 11-4*
- *Système de détection d'intrusion à la page 11-4*
- *Surveillance des épidémies de violation de pare-feu à la page 11-6*
- *Privilèges du pare-feu clients OfficeScan à la page 11-6*

Filtrage du trafic

Le pare-feu OfficeScan filtre l'ensemble du trafic entrant et sortant, permettant ainsi de bloquer certains types de trafic sur la base des critères suivants :

- Direction (entrant/sortant)
- Protocole (TCP/UDP/ICMP/ICMPv6)
- Ports de destination
- Ordinateurs source et de destination

Filtrage d'applications

Le pare-feu OfficeScan filtre le trafic entrant et sortant de certaines applications, permettant à ces dernières d'accéder au réseau. Cependant, les connexions réseau dépendront des stratégies définies par l'administrateur.

Liste Certified Safe Software

La liste Certified Safe Software fournit une liste d'applications qui peuvent contourner les niveaux de sécurité de la stratégie de pare-feu. Si le niveau de sécurité est défini à Moyen ou Élevé, OfficeScan permettra tout de même aux applications de s'exécuter et d'accéder au réseau.

Activez l'interrogation de la liste Certified Safe Software globale qui s'avère plus complète. Il s'agit d'une liste que Trend Micro met à jour de manière dynamique.

Remarque

Cette fonctionnalité utilise la surveillance des comportements. Vérifiez que le service de prévention des modifications non autorisées et Certified Safe Software Service ont été activés avant d'activer la liste Liste Certified Safe Software globale.

Recherche de virus de réseau

Le pare-feu OfficeScan vérifie également la présence de virus de réseau dans chaque paquet. Pour obtenir des informations détaillées, voir *Virus de réseau à la page 6-3*.

Profils et stratégies personnalisables

Le pare-feu OfficeScan vous permet de configurer des stratégies destinées à bloquer ou à autoriser certains types de trafic réseau. Attribuez une stratégie à un ou plusieurs profils que vous pouvez ensuite déployer à des clients OfficeScan. Vous disposez ainsi d'une méthode d'organisation et de configuration personnalisée des paramètres de pare-feu des clients.

Stateful Inspection

Le pare-feu OfficeScan est de type Stateful inspection : il contrôle toutes les connexions au client OfficeScan et mémorise tous les états de connexion. Il peut identifier les conditions spécifiques de toute connexion, prédire les actions qui doivent être effectuées et détecter toute anomalie de connexion. L'utilisation efficace du pare-feu repose donc non seulement sur la création de profils et de stratégies, mais aussi sur l'analyse des connexions et le filtrage des paquets qui transitent par le pare-feu.

Système de détection d'intrusion

Le pare-feu OfficeScan comprend également un système de détection d'intrusion (SDI). Lorsqu'il est activé, le SDI peut contribuer à identifier des signatures dans les paquets réseau indiquant une attaque du client OfficeScan. Le pare-feu OfficeScan peut empêcher les intrusions bien connues suivantes :

- **Fragment trop important** : Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet TCP/UDP surdimensionné sur un ordinateur cible. Par conséquent, la mémoire tampon des ordinateurs peut déborder, ce qui risque de geler ou de redémarrer la machine.
- **Ping of Death** : Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet ICMP/ICMPv6 surdimensionné sur un ordinateur cible. Par conséquent, la mémoire tampon des ordinateurs peut déborder, ce qui risque de geler ou de redémarrer la machine.
- **ARP conflictuel** : Type d'attaque dans le cadre de laquelle un pirate envoie à un ordinateur une requête de protocole de résolution d'adresse (Address Resolution Protocol ou ARP) avec des adresses IP source et de destination identiques.

L'ordinateur cible s'envoie continuellement une réponse ARP (son adresse MAC) et dès lors gèle ou se plante.

- **SYN Flood** : Attaque de refus de service dans le cadre de laquelle un programme envoie plusieurs paquets de synchronisation TCP (SYN) à un ordinateur, celui-ci envoyant alors continuellement des réponses d'accusé-réception de synchronisation (SYN/ACK). Cela peut épuiser la mémoire d'un ordinateur et finalement bloquer l'ordinateur.

- **Fragment de chevauchement** : Similaire à une attaque Teardrop, cette attaque de refus de service envoie des fragments TCP de chevauchement à un ordinateur. Par conséquent, les informations de l'en-tête sont écrasées dans le premier fragment TCP qui risque alors de passer à travers le pare-feu. Le pare-feu peut ensuite autoriser les fragments suivants contenant du code malicieux à se frayer un chemin vers l'ordinateur cible.

- **Teardrop** : Similaire à une attaque de fragment de chevauchement, cette attaque de refus de service a trait à des fragments IP. Une valeur de décalage prêtant à confusion dans le deuxième fragment IP ou dans un fragment ultérieur peut provoquer le blocage du système d'exploitation de l'ordinateur récepteur lorsque celui-ci tente de réassembler les fragments.

- **Attaque par fragment minuscule** : Avec ce type d'attaque, un fragment TCP de petite taille force la première en-tête de paquet TCP dans le fragment suivant. Cela peut amener les routeurs filtrant le trafic à ignorer les fragments suivants qui peuvent contenir des données malveillantes.

- **IGMP fragmenté** : Attaque de refus de service qui envoie des paquets d'IGMP fragmentés à un ordinateur cible, lequel ne peut pas les traiter correctement. Cela peut geler ou ralentir l'ordinateur.

- **Attaque LAND** : Type d'attaque qui envoie à un ordinateur des paquets de synchronisation IP (SYN) dont les adresses source et cible sont identiques. Celui-ci s'envoie alors en retour un accusé-réception de la synchronisation (SYN/ACK). Cela peut geler ou ralentir l'ordinateur.

Surveillance des épidémies de violation de pare-feu

Le pare-feu OfficeScan envoie un message de notification à des destinataires spécifiés lorsque le nombre de violations de pare-feu dépasse un seuil déterminé, ce qui peut constituer un signal d'attaque.

Privilèges du pare-feu clients OfficeScan

Accordez aux utilisateurs clients OfficeScan le privilège d'afficher leurs paramètres de pare-feu sur la console du client OfficeScan. Vous pouvez également accorder aux utilisateurs le privilège d'activation ou de désactivation du pare-feu, du système de détection d'intrusion et du message de notification de violation du pare-feu.

Activation ou désactivation du pare-feu OfficeScan

Pendant l'installation du serveur OfficeScan, vous êtes invité à activer ou désactiver le pare-feu OfficeScan.

Si vous avez activé le pare-feu pendant l'installation et remarqué que les performances en avaient été affectées, notamment sur les plates-formes serveur (Windows Server 2003 et Windows Server 2008), désactivez le pare-feu.

Si vous avez désactivé le pare-feu pendant l'installation mais que vous souhaitez l'activer par la suite afin de protéger un client des intrusions, lisez d'abord les conseils et instructions dans *Services du client OfficeScan à la page 13-7*.

Vous pouvez activer ou désactiver le pare-feu sur l'ensemble des ordinateurs du client OfficeScan ou sur certains d'entre eux.

Activation ou désactivation du pare-feu OfficeScan sur les ordinateurs sélectionnés

Méthode A : Créez une nouvelle stratégie et appliquez-la aux clients OfficeScan.

Tâche

1. Créez une stratégie qui active/désactive le pare-feu. Pour connaître les étapes de création d'une stratégie, voir *Ajout ou modification d'une stratégie de pare-feu à la page 11-11*.
2. Appliquez la stratégie aux clients OfficeScan.

Méthode B : Activez/désactivez le pilote et le service de pare-feu.

Tâche

1. Activez/désactivez le pilote de pare-feu.
   a. Ouvrez les **propriétés de connexion au réseau Windows**.
   b. Cochez ou décochez la case **Pilote du pare-feu commun Trend Micro** pour la carte réseau.
2. Activez/désactivez le service de pare-feu.
   a. Ouvrez une invite de commande et entrez `services.msc`.
   b. Démarrez ou arrêtez le **Pare-feu d'OfficeScan NT** dans Microsoft Management Console (MMC).

Méthode C : Activez/désactivez le service de pare-feu de la console Web

Pour les étapes détaillées, voir *Services du client OfficeScan à la page 13-7*.

Activation ou désactivation du pare-feu OfficeScan sur tous les ordinateurs

Tâche

1. Accédez à **Administration** > **Product License**.
2. Accédez à la section **Services complémentaires**.
3. Dans la section **Services complémentaires**, à côté du pare-feu pour les ordinateurs en réseau, cliquez sur **Activer** ou sur **Désactiver**.

Stratégies et profils de pare-feu

Le pare-feu OfficeScan utilise des stratégies et des profils pour organiser et personnaliser des méthodes de protection des ordinateurs en réseau.

Avec l'intégration d'Active Directory et de l'administration basée sur les rôles, chaque rôle d'utilisateur, selon les autorisations associées, peut créer, configurer ou supprimer des stratégies et des profils pour des domaines spécifiques.

Conseil

Plusieurs installations de pare-feu sur le même ordinateur peuvent produire des résultats inattendus. Envisagez de désinstaller les autres applications de pare-feu logicielles sur les clients OfficeScan avant de déployer et d'activer le pare-feu OfficeScan.

Les étapes suivantes sont nécessaires pour utiliser correctement le pare-feu OfficeScan :

1. Créez une stratégie. Une stratégie vous permet de sélectionner un niveau de sécurité qui bloque ou autorise le trafic sur les ordinateurs en réseau et active les fonctions du pare-feu.
2. Ajoutez des exceptions à la stratégie. Les exceptions permettent aux clients OfficeScan de dévier d'une stratégie. Grâce aux exceptions, vous pouvez spécifier des clients et autoriser ou bloquer certains types de trafic malgré le niveau de sécurité défini dans la stratégie. Par exemple, vous pouvez bloquer tout le trafic

pour un ensemble de clients dans une stratégie, mais créer une exception qui autorise le trafic HTTP pour que les clients puissent accéder à un serveur Web.

3. Créez et attribuez des profils aux clients OfficeScan. Un profil de pare-feu, qui comprend un ensemble d'attributs clients, est associé à une stratégie. Une fois qu'un client correspond aux attributs spécifiés dans le profil, la stratégie associée est déclenchée.

Stratégies de pare-feu

Les stratégies de pare-feu vous permettent de bloquer ou d'autoriser certains types de trafic réseau non spécifiés dans une exception de stratégie. Une stratégie définit également les fonctions de pare-feu qui sont activées ou désactivées. Attribuez une stratégie à un ou plusieurs profils de pare-feu.

OfficeScan est fourni avec un ensemble de stratégies par défaut, que vous pouvez modifier ou supprimer.

Avec l'intégration d'Active Directory et de l'administration basée sur les rôles, chaque rôle d'utilisateur, selon les autorisations associées, peut créer, configurer ou supprimer des stratégies pour des domaines spécifiques.

Le tableau suivant répertorie les stratégies de pare-feu par défaut.

TABLEAU 11-1. Stratégies de pare-feu par défaut

NOM DE LA STRATÉGIE	NIVEAU DE SÉCURITÉ	PARAMÈTRES CLIENT	EXCEPTIONS	UTILISATION RECOMMANDÉE
Tous les accès	Faible	Activer le pare-feu	Aucune	À utiliser pour permettre aux clients un accès illimité au réseau
Cisco Trust Agent pour Cisco NAC	Faible	Activer le pare-feu	Autoriser le trafic UDP entrant/sortant via le port 21862	À utiliser lorsque les clients ont une installation Cisco Trust Agent (CTA)

NOM DE LA STRATÉGIE	NIVEAU DE SÉCURITÉ	PARAMÈTRES CLIENT	EXCEPTIONS	UTILISATION RECOMMANDÉE
Ports de communication pour Trend Micro Control Manager	Faible	Activer le pare-feu	Autoriser tout le trafic TCP/UDP entrant/sortant via les ports 80 et 10319	À utiliser lorsque les clients ont une installation d'agent MCP
Console ScanMail for Microsoft Exchange	Faible	Activer le pare-feu	Autoriser tout le trafic TCP entrant/ sortant via le port 16372	À utiliser lorsque les clients veulent accéder à la console ScanMail
Console InterScan Messaging Security Suite (IMSS)	Faible	Activer le pare-feu	Autoriser tout le trafic TCP entrant/ sortant via le port 80	À utiliser lorsque les clients veulent accéder à la console IMSS

Créez également de nouvelles stratégies si vous avez des besoins non couverts par les stratégies par défaut.

Toutes les stratégies par défaut et créées par l'utilisateur s'affichent dans la liste des stratégies du pare-feu sur la console Web.

Configuration de la liste des stratégies du pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies**.
2. Pour ajouter une nouvelle stratégie, cliquez sur **Ajouter**.

   Si la nouvelle stratégie que vous souhaitez créer possède des paramètres similaires à ceux d'une stratégie existante, sélectionnez cette dernière et cliquez sur **Copier**. Pour modifier une stratégie existante, cliquez sur son nom.

   Un écran de configuration de stratégie s'affiche. Voir la *Ajout ou modification d'une stratégie de pare-feu à la page 11-11* pour plus d'informations.

3. Pour supprimer une stratégie existante, cochez la case en regard de la stratégie, puis cliquez sur **Supprimer**.

4. Pour modifier le modèle d'exception du pare-feu, cliquez sur **Modifier le modèle d'exception**.

   Voir la *Modification du modèle d'exception du pare-feu à la page 11-14* pour plus d'informations.

   L'éditeur de modèle d'exception apparaît.

Ajout ou modification d'une stratégie de pare-feu

Configurez ce qui suit pour chaque stratégie :

- **Niveau de sécurité** : Paramètre général qui bloque ou autorise tout le trafic entrant et/ou sortant sur l'ordinateur client OfficeScan.
- **Fonctionnalités du pare-feu** : Déterminez s'il convient d'activer ou de désactiver le pare-feu OfficeScan, le Système de détection d'intrusion (IDS) et le message de notification de violation de pare-feu. Voir *Système de détection d'intrusion à la page 11-4* pour obtenir des informations complémentaires sur SDI.
- **Liste Certified Safe Software** : spécifiez si vous souhaitez autoriser les applications certifiées comme sécurisées à se connecter au réseau. Voir *Liste Certified Safe Software à la page 11-3* pour obtenir des informations complémentaires sur la Liste Certified Safe Software.
- **Liste des exceptions de stratégie** : Liste d'exceptions configurables qui permet de bloquer ou d'accepter différents types de trafic réseau.

Ajout d'une stratégie de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies**.

2. Pour ajouter une nouvelle stratégie, cliquez sur **Ajouter**.

   Si vous souhaitez créer une stratégie possédant des paramètres semblables à ceux d'une stratégie existante, sélectionnez cette dernière et cliquez sur **Copier**.

3. Entrez un nom pour la stratégie.

4. Sélectionnez un niveau de sécurité.

   Le niveau de sécurité sélectionné ne s'applique pas au trafic répondant aux critères de l'exception de stratégie du pare-feu.

5. Sélectionnez les fonctions du pare-feu à utiliser pour la stratégie.

   - Le message de notification de violation du pare-feu s'affiche lorsque le pare-feu bloque un paquet sortant. Pour modifier le message, reportez-vous à *Modification du contenu du message de notification de pare-feu à la page 11-30*.

   - L'activation de toutes les fonctionnalités du pare-feu confère aux utilisateurs du client OfficeScan les privilèges d'activation/de désactivation des fonctions et de modification des paramètres du pare-feu dans la console client OfficeScan.

     AVERTISSEMENT!

     Vous ne pouvez pas utiliser la console Web du serveur OfficeScan pour écraser les paramètres de la console client OfficeScan configurés par l'utilisateur.

   - Si vous n'activez pas ces fonctionnalités, les paramètres du pare-feu que vous configurez à partir de la console Web du serveur OfficeScan s'affichent sous Liste des cartes réseau sur la console client OfficeScan.

   - Les informations affichées sous **Paramètres**, sous l'onglet **Pare-feu** de la console client OfficeScan, reflètent toujours les paramètres configurés à partir de la console client OfficeScan et non de la console Web du serveur.

6. Activez la liste Certified Safe Software locale ou globale.

   Remarque

   Vérifiez que le service de prévention des modifications non autorisées et Certified Safe Software Services ont été activés avant d'activer ce service.

7. Sous Exception, sélectionnez les exceptions de stratégie de pare-feu. Les exceptions de stratégie répertoriées sont basées sur le modèle d'exception de pare-feu. Voir *Modification du modèle d'exception du pare-feu à la page 11-14* pour obtenir des informations détaillées.

- Modifiez une exception de stratégie existante en cliquant sur son nom et en modifiant les paramètres dans la page qui s'affiche.

  Remarque

  L'exception de stratégie modifiée ne s'appliquera qu'à la stratégie créée ultérieurement. Si vous souhaitez que la modification d'exception de stratégie soit permanente, vous devez apporter la même modification à l'exception de stratégie dans le modèle d'exception de pare-feu.

- Cliquez sur **Ajouter** pour créer une nouvelle exception de stratégie. Spécifiez les paramètres dans la page qui s'affiche.

  Remarque

  L'exception de stratégie ne s'appliquera également qu'à la stratégie créée ultérieurement. Pour appliquer cette exception de stratégie à d'autres stratégies, vous devez d'abord l'ajouter à la liste des exceptions de stratégies dans le modèle d'exception du pare-feu.

8. Cliquez sur **Enregistrer**.

Modification d'une stratégie de pare-feu existante

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies**.
2. Cliquez sur une stratégie.
3. Modifiez ce qui suit :
   - Nom de la stratégie
   - Niveau de sécurité
   - Fonctions du pare-feu à utiliser pour la stratégie
   - État de la liste Certified Safe Software Service
   - Exceptions de stratégie de pare-feu à inclure à la stratégie

- Modifiez une exception de stratégie existante (cliquez sur le nom de l'exception de stratégie et modifiez les paramètres dans la page qui s'affiche)
- Cliquez sur **Ajouter** pour créer une nouvelle exception de stratégie. Spécifiez les paramètres dans la page qui s'affiche.

4. Cliquez sur **Enregistrer** pour appliquer les modifications à la stratégie existante.

Modification du modèle d'exception du pare-feu

Le modèle d'exception du pare-feu contient des exceptions de stratégie que vous pouvez configurer de manière à autoriser ou à bloquer divers types de trafic réseau à partir des numéros de port et des adresses IP de l'ordinateur du client OfficeScan. Lorsque vous avez créé une exception de stratégie, modifiez les stratégies auxquelles elle s'applique.

Choisissez le type d'exception de stratégie que vous voulez utiliser. Deux types sont proposés :

- **Les exceptions restrictives**

  Elles bloquent uniquement les types spécifiés de trafic réseau et s'appliquent aux stratégies qui autorisent tout le trafic réseau. Un exemple d'utilisation d'une exception de stratégie restrictive est de bloquer les ports clients OfficeScan vulnérables aux attaques, tels que les ports souvent utilisés par les chevaux de Troie.

- **Les exceptions permissives**

  Elles autorisent uniquement les types spécifiés de trafic réseau et s'appliquent aux stratégies qui bloquent tout le trafic réseau. Par exemple, lorsque vous souhaitez autoriser des clients OfficeScan à accéder uniquement au serveur OfficeScan et à un serveur Web. Pour cela, autorisez le trafic depuis le port sécurisé (utilisé pour communiquer avec le serveur OfficeScan) et le port que le client OfficeScan utilise pour la communication HTTP.

  Port d'écoute du client OfficeScan : **Ordinateurs en réseau** > **Paramètres clients généraux > État**. Le numéro de port se trouve sous **Informations de base**.

Port d'écoute du serveur : **Administration** > **Paramètres de connexion**. Le numéro de port se trouve sous **Paramètres de connexion pour les ordinateurs en réseau**.

OfficeScan est fourni avec un ensemble d'exceptions de stratégie de pare-feu par défaut, que vous pouvez modifier ou supprimer.

TABLEAU 11-2. Exceptions de stratégie de pare-feu par défaut

NOM DE L'EXCEPTION	ACTION	PROTOCOLE	PORT	DIRECTION
DNS	Autoriser	TCP/UDP	53	Entrant et sortant
NetBIOS	Autoriser	TCP/UDP	137, 138, 139, 445	Entrant et sortant
HTTPS	Autoriser	TCP	443	Entrant et sortant
HTTP	Autoriser	TCP	80	Entrant et sortant
Telnet	Autoriser	TCP	23	Entrant et sortant
SMTP	Autoriser	TCP	25	Entrant et sortant
FTP	Autoriser	TCP	21	Entrant et sortant
POP3	Autoriser	TCP	110	Entrant et sortant
LDAP	Autoriser	TCP/UDP	389	Entrant et sortant

Remarque

Les exceptions par défaut s'appliquent à tous les clients. Si vous souhaitez qu'une exception par défaut s'applique à certains clients seulement, modifiez-la et indiquez les adresses IP des clients.

L'exception LDAP n'est pas disponible si vous effectuez une mise à niveau à partir d'une version précédente d'OfficeScan. Ajoutez cette exception manuellement si vous ne la voyez pas dans la liste d'exceptions.

Ajout d'une exception de stratégie de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies**.
2. Cliquez sur **Modifier le modèle d'exception**.
3. Cliquez sur **Ajouter**.
4. Entrez un nom pour l'exception de stratégie.
5. Sélectionnez le type d'application. Vous pouvez sélectionner toutes les applications ou spécifier un chemin d'application ou des clés de registre.

   Remarque

   Vérifiez le nom et les chemins complets saisis. L'exception d'application ne prend pas en charge les caractères génériques.

6. Sélectionnez l'action qu'OfficeScan effectuera sur le trafic réseau (bloquer ou autoriser le trafic qui répond au critère d'exception) et le sens du trafic (trafic réseau entrant ou sortant sur l'ordinateur client OfficeScan).
7. Sélectionnez le type de protocole réseau : TCP, UDP, ICMP ou ICMPv6.
8. Spécifiez les ports de l'ordinateur client OfficeScan sur lesquels vous souhaitez exécuter l'action.
9. Sélectionnez les adresses IP de l'ordinateur client OfficeScan à inclure dans l'exception. Par exemple, si vous choisissez de refuser tout le trafic réseau (entrant et sortant) et que vous saisissez l'adresse IP d'un ordinateur unique sur le réseau, les

clients OfficeScan dont la stratégie contient cette exception ne pourront pas envoyer de données vers cette adresse IP ou en recevoir à partir de celle-ci.

- **Toutes les adresses IP** : comprend toutes les adresses IP
- **Adresse IP unique** : saisissez une adresse IPv4 ou IPv6, ou un nom d'hôte.
- **Plage (pour IPv4 ou IPv6)** : Saisissez une plage d'adresses IPv4 ou IPv6.
- **Plage (pour IPv6)** : Saisissez le préfixe et la longueur d'une adresse IPv6.
- **Masque de sous-réseau** : Saisissez une adresse IPv4 et son masque de sous-réseau.

10. Cliquez sur **Enregistrer**.

Modification d'une exception de stratégie de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies**.
2. Cliquez sur **Modifier le modèle d'exception**.
3. Cliquez sur une exception de stratégie.
4. Modifiez ce qui suit :
   - Nom de l'exception de stratégie
   - Type, nom ou chemin de l'application
   - Action qu'OfficeScan effectuera sur le trafic réseau et direction du trafic
   - Le type de protocole réseau
   - Les numéros de port de l'exception de stratégie
   - Les adresses IP des ordinateurs clients OfficeScan
5. Cliquez sur **Enregistrer**.

Enregistrement des paramètres de la liste d'exceptions de stratégie

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies**.
2. Cliquez sur **Modifier le modèle d'exception**.
3. Cliquez sur l'une des options d'enregistrement suivantes :
   - **Enregistrer les modifications du modèle** : enregistre le modèle d'exception avec les exceptions de stratégie et les paramètres actuels. Cette option n'applique le modèle d'exception qu'aux stratégies créées ultérieurement, pas aux stratégies existantes.
   - **Enregistrer et appliquer aux stratégies existantes** : enregistre le modèle d'exception avec les exceptions de stratégie et les paramètres actuels. Cette option applique le modèle aux stratégies existantes et futures.

Profils de pare-feu

Les profils de pare-feu offrent une flexibilité en vous permettant de sélectionner les attributs dont doit disposer un client ou un groupe de clients avant d'appliquer une stratégie. Créez des rôles utilisateur qui peuvent créer, configurer ou supprimer des profils pour des domaines spécifiques.

Les utilisateurs se servant du compte utilisateurs intégré ou ceux disposant d'autorisations de gestion complètes, peuvent également activer l'option **Remplacer la liste d'exceptions du niveau de sécurité du client** pour remplacer les paramètres du profil client OfficeScan par les paramètres du serveur.

Les profils incluent les options suivantes :

- **Stratégie associée** : Chaque profil utilise une stratégie unique
- **Attributs client** : Les clients OfficeScan disposant d'un ou de plusieurs des attributs suivants appliquent la stratégie associée°:
  - **Adresse IP** : Un client OfficeScan disposant d'une adresse IP spécifique, d'une adresse IP comprise dans une plage d'adresses IP ou d'une adresse IP appartenant à un sous-réseau spécifié

- **Domaine** : Un client OfficeScan appartenant à un domaine OfficeScan déterminé
- **Ordinateur** : Un client OfficeScan associé à un nom d'ordinateur spécifique
- **Plate-forme** : Un client OfficeScan client exécutant une plate-forme spécifique
- **Nom de connexion** : Les ordinateurs client OfficeScan auxquels les utilisateurs spécifiés se sont connectés
- **Description de la carte d'interface réseau** : Un client OfficeScan associé à une description de carte d'interface réseau correspondante
- **État de la connexion client** : Si un client OfficeScan est connecté ou déconnecté

Remarque

Un client OfficeScan est connecté lorsqu'il peut se connecter au serveur OfficeScan ou à l'un des serveurs de référence, et déconnecté s'il ne peut se connecter à aucun serveur.

- Privilèges utilisateur : Permettent ou empêchent les utilisateurs du client OfficeScan d'effectuer les opérations suivantes :
  - Modification du niveau de sécurité spécifié dans une stratégie
  - Modification de la liste des exceptions associée à une stratégie

Remarque

Ces privilèges s'appliquent uniquement aux clients qui correspondent aux attributs spécifiés dans le profil. Vous pouvez affecter les autres privilèges de pare-feu à certains utilisateurs du client. Voir *Privilèges du pare-feu à la page 11-24* pour obtenir des informations détaillées.

OfficeScan est fourni avec un profil par défaut nommé « Tous les profils clients » utilisant la stratégie « Tous les accès ». Vous pouvez modifier ou supprimer ce profil par défaut. Vous pouvez aussi créer de nouveaux profils. Tous les profils de pare-feu par défaut et créés par l'utilisateur, y compris la stratégie associée à chaque profil et l'état du profil actuel, s'affichent sur la liste des profils du pare-feu sur la console Web. Gérez la

liste des profils et déployez tous les profils sur les clients OfficeScan. Les clients OfficeScan enregistrent tous les profils du pare-feu sur l'ordinateur client.

Configuration de la liste des profils du pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Profils**.
2. Les utilisateurs se servant du compte d'administrateur intégré, ou ceux disposant des autorisations de gestion complètes, peuvent éventuellement activer l'option **Remplacer la liste d'exceptions du niveau de sécurité du client** pour remplacer les paramètres du profil client OfficeScan par les paramètres du serveur.
3. Pour ajouter un nouveau profil, cliquez sur **Ajouter**. Pour modifier un profil existant, sélectionnez son nom.

   Un écran de configuration de profil s'affiche. Voir *Ajout et modification d'un profil du pare-feu à la page 11-22* pour plus d'informations.
4. Pour supprimer une stratégie existante, cochez la case en regard de la stratégie, puis cliquez sur **Supprimer**.
5. Pour modifier l'ordre des profils dans la liste, cochez la case en regard du profil à déplacer, puis cliquez sur **Monter** ou **Descendre**.

   OfficeScan applique les profils du pare-feu aux clients OfficeScan dans l'ordre dans lequel les profils apparaissent dans la liste. Par exemple, si un client correspond au premier profil, OfficeScan applique au client les actions configurées pour ce profil. Les autres profils également configurés pour ce client sont ignorés par OfficeScan.

   Conseil

   Placez les stratégies les plus exclusives au sommet de la liste. Placez par exemple une stratégie que vous créez pour un client unique au sommet de la liste, suivies des stratégies qui concernent une gamme de clients, un domaine réseau, puis enfin celles qui concernent tous les clients.
6. Pour gérer les serveurs de référence, cliquez sur **Modifier la liste de serveurs de référence**. Les serveurs de référence sont des ordinateurs qui remplacent le serveur OfficeScan lors de l'application des profils de pare-feu. Un serveur de référence

peut être n'importe quel ordinateur se trouvant sur le réseau (voir *Serveurs de référence à la page 12-30* pour plus d'infomations). OfficeScan suppose que les conditions suivantes sont remplies lorsque vous activez des serveurs de référence :

- Les clients OfficeScan connectés à des serveurs de référence sont en ligne, même si les clients ne peuvent pas communiquer avec le serveur OfficeScan.
- Les profils du pare-feu appliqués à des clients OfficeScan connectés s'appliquent également aux clients OfficeScan connectés à des serveurs de référence.

Remarque

Seuls les utilisateurs du compte d'administrateur intégré ou ceux disposant d'autorisations de gestion complètes peuvent voir et configurer la liste des serveurs de référence.

7. Pour enregistrer les paramètres actuels et attribuer les profils aux clients OfficeScan :
   a. Sélectionnez ou non l'option **Remplacer le niveau de sécurité/la liste d'exceptions du client**. Cette option écrase tous les paramètres de pare-feu configurés par l'utilisateur.
   b. Cliquez sur **Affecter un profil aux clients**. OfficeScan attribue à tous les clients OfficeScan l'ensemble des profils figurant dans la liste.
8. Pour vérifier que les profils ont été correctement attribués aux clients OfficeScan :
   a. Accédez à **Ordinateurs en réseau** > **Gestion des clients**. Sélectionnez **Pare-feu** dans la liste déroulante d'affichage de l'arborescence des clients.
   b. Vérifiez la présence d'une coche verte dans la colonne **Pare-feu** de l'arborescence des clients. Si la stratégie associée au profil autorise le système de détection d'intrusion, une coche verte s'affiche également dans la colonne **SDI**.
   c. Vérifiez que le client applique la bonne stratégie de pare-feu. La stratégie apparaît dans la colonne **Stratégie de pare-feu** dans l'arborescence des clients.

Ajout et modification d'un profil du pare-feu

Les ordinateurs client OfficeScan peuvent exiger différents niveaux de protection. Les profils du pare-feu vous permettent de préciser les ordinateurs clients auxquels s'applique une stratégie associée et d'accorder aux utilisateurs clients des privilèges leur permettant de modifier les paramètres du pare-feu. Généralement, un profil par stratégie utilisée est nécessaire.

Ajout d'un profil de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Profils**.
2. Cliquez sur **Ajouter**.
3. Cliquez sur **Activer ce profil** pour qu'OfficeScan puisse déployer ce profil vers les clients OfficeScan.
4. Saisissez un nom d'identification du profil, ainsi qu'une description facultative.
5. Sélectionnez une stratégie pour ce profil.
6. Spécifiez les ordinateurs clients auxquels OfficeScan applique la stratégie. Sélectionnez les ordinateurs en fonction des critères suivants :
   - adresse IP
   - Domaine : cliquez sur ce bouton pour ouvrir l'arborescence client et sélectionner des domaines.

     Remarque

     Seuls les utilisateurs disposants d'autorisations complètes sur les domaines peuvent sélectionner des domaines.
   - Nom de l'ordinateur : Cliquez sur ce bouton puis sélectionnez les ordinateurs client OfficeScan, pour ouvrir l'arborescence client.
   - Plate-forme
   - Nom de connexion

- Description de la carte d'interface réseau : Saisissez une description complète ou partielle, sans caractères de substitution.

Conseil

Trend Micro recommande de saisir le fabricant de la carte d'interface réseau (NIC) car les descriptions NIC commencent en général par le nom du fabricant. Par exemple, si vous avez saisi « Intel », toutes les cartes d'interface réseau fabriquées par Intel rempliront les critères. Si vous avez saisi un modèle de carte d'interface réseau particulier, par exemple « Intel(R) Pro/100 », seules les descriptions NIC commençant par « Intel(R) Pro/100 » rempliront les critères.

- État de la connexion client

7. Choisissez d'accorder aux utilisateurs le privilège de modification du niveau de sécurité du pare-feu ou de modification d'une liste configurable d'exceptions pour autoriser les types de trafic spécifiés.

   Consultez la rubrique *Ajout ou modification d'une stratégie de pare-feu à la page 11-11* pour obtenir de plus amples informations sur ces options.

8. Cliquez sur **Enregistrer**.

Modification d'un profil de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Profils**.
2. Cliquez sur un profil.
3. Cliquez sur **Activer ce profil** pour qu'OfficeScan puisse déployer ce profil vers les clients OfficeScan. Modifiez ce qui suit :
   - Le nom et la description du profil
   - La stratégie attribuée au profil
   - Les ordinateurs clients OfficeScan, basés sur les critères suivants :
     - adresse IP

- Domaine : cliquez sur ce bouton pour ouvrir l'arborescence des clients et sélectionner des domaines.
- Nom de l'ordinateur : cliquez sur ce bouton pour ouvrir l'arborescence des clients et sélectionner des ordinateurs clients.
- Plate-forme
- Nom de connexion
- Description de la carte d'interface réseau : Saisissez une description complète ou partielle, sans caractères de substitution.

  Conseil

  Trend Micro recommande de saisir le fabricant de la carte d'interface réseau (NIC) car les descriptions NIC commencent en général par le nom du fabricant. Par exemple, si vous avez saisi « Intel », toutes les cartes d'interface réseau fabriquées par Intel rempliront les critères. Si vous avez saisi un modèle de carte d'interface réseau particulier, par exemple « Intel(R) Pro/100 », seules les descriptions NIC commençant par « Intel(R) Pro/100 » rempliront les critères.

- État de la connexion client

- Privilèges : Choisissez d'accorder aux utilisateurs le privilège de modification du niveau de sécurité du pare-feu ou de modification d'une liste configurable d'exceptions pour autoriser les types de trafic spécifiés. Consultez la rubrique *Ajout ou modification d'une stratégie de pare-feu à la page 11-11* pour obtenir de plus amples informations sur ces options.

4. Cliquez sur **Enregistrer**.

Privilèges du pare-feu

Autorisent les utilisateurs à configurer leurs propres paramètres de pare-feu. Tous les paramètres configurés par l'utilisateur ne peuvent pas être remplacés par des paramètres déployés à partir du serveur OfficeScan. Par exemple, si l'utilisateur désactive le système

de détection d'intrusion (IDS) et si vous activez IDS sur le serveur OfficeScan, IDS reste désactivé sur l'ordinateur client OfficeScan.

Activez les paramètres suivant pour permettre aux utilisateurs de configurer le pare-feu :

- **Afficher l'onglet Pare-feu sur la console client**

  L'onglet **Pare-feu** affiche tous les paramètres de pare-feu sur le client OfficeScan et permet aux utilisateurs disposant de privilèges de pare-feu de configurer leurs propres paramètres.

- **Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu**

  Le pare-feu OfficeScan protège les clients et les serveurs du réseau grâce à une fonction Stateful inspection, à un scan antivirus de réseau haute performance et à l'élimination des virus de réseau. Si vous accordez aux utilisateurs le privilège d'activer ou de désactiver le pare-feu et ses fonctionnalités, avertissez-les de ne pas désactiver le pare-feu trop longtemps pour éviter d'exposer l'ordinateur aux intrusions et aux attaques de pirates.

  Si vous n'accordez pas ces privilèges aux utilisateurs, les paramètres du pare-feu que vous configurez depuis la console Web du serveur OfficeScan s'affichent sous Liste des cartes réseau sur la console du client OfficeScan.

- **Autoriser les clients à envoyer les journaux de pare-feu au serveur OfficeScan**

  Sélectionnez cette option pour analyser le trafic que le pare-feu OfficeScan bloque et autorise. Pour plus d'informations sur les journaux de pare-feu, voir *Journaux de pare-feu à la page 11-30*.

  Si vous sélectionnez cette option, configurez la programmation d'envoi de journaux dans **Ordinateurs en réseau** > **Gestion des clients**. Rendez-vous à la section **Paramètres du pare-feu**. La programmation ne s'applique qu'aux clients disposant du privilège d'envoi des journaux de pare-feu. Pour des instructions, voir *Paramètres généraux du pare-feu à la page 11-27*.

Accord des privilèges de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges du pare-feu**.
5. Sélectionnez les options suivantes :
   - *Afficher l'onglet Pare-feu sur la console client à la page 11-25*
   - *Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu à la page 11-25*
   - *Autoriser les clients à envoyer les journaux de pare-feu au serveur OfficeScan à la page 11-25*
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Paramètres généraux du pare-feu

Les paramètres généraux du pare-feu peuvent être appliqués aux clients OfficeScan de diverses manières.

- Un paramètre particulier du pare-feu peut être appliqué à tous les clients gérés par le serveur.
- Il est possible qu'un paramètre ne s'applique au client OfficeScan que selon certains privilèges du pare-feu. Par exemple, le journal de pare-feu envoyant une programmation ne s'applique qu'aux clients OfficeScan ayant le privilège d'envoyer des journaux au serveur.

Activez les paramètres généraux suivants selon vos besoins :

- **Envoyer des journaux de pare-feu au serveur**

  Vous pouvez accorder à certains clients OfficeScan le privilège d'envoyer des journaux de pare-feu au serveur OfficeScan. Configurez la programmation d'envoi de journaux dans cette section. Seuls les clients bénéficiant du privilège d'envoi de journaux de pare-feu peuvent utiliser cette programmation.

  Voir *Privilèges du pare-feu à la page 11-24* pour obtenir des informations relatives aux privilèges de pare-feu disponibles pour les clients sélectionnés.

- **Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système**

  Activez le client OfficeScan pour mettre à jour Pilote du pare-feu commun uniquement après le redémarrage de l'ordinateur du client OfficeScan. Activez cette option pour éviter des anomalies potentielles sur l'ordinateur client (telles qu'une déconnexion temporaire du réseau) lorsque le pilote du pare-feu commun se met à jour pendant une mise à niveau du client.

  Remarque

  Cette fonction n'est disponible que pour les clients disposant des versions OfficeScan 8.0 SP1 et ultérieures.

- **Envoyer au serveur OfficeScan les informations du journal du pare-feu toutes les heures pour déterminer si une épidémie du pare-feu survient**

Lorsque vous activez cette option, les clients OfficeScan communiquent une fois par heure au serveur OfficeScan le nombre d'entrées du journal du pare-feu. Pour plus d'informations sur les journaux de pare-feu, voir *Journaux de pare-feu à la page 11-30*.

OfficeScan utilise le nombre d'entrée des journaux et les critères liés aux épidémies de violation du pare-feu pour déterminer si une épidémie du pare-feu survient. Lors d'une épidémie, OfficeScan envoie des notifications par courrier électronique aux administrateurs OfficeScan.

Configuration des paramètres généraux de pare-feu

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Allez aux sections suivantes et configurez les paramètres :

TABLEAU 11-3. Paramètres généraux du pare-feu

SECTION	PARAMÈTRES
Paramètres du pare-feu	• *Envoyer des journaux de pare-feu au serveur à la page 11-27* • *Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système à la page 11-27*
Nombre d'entrées du journal du pare-feu	*Envoyer au serveur OfficeScan les informations du journal du pare-feu toutes les heures pour déterminer si une épidémie du pare-feu survient à la page 11-27*

3. Cliquez sur **Enregistrer**.

Notifications de violation du pare-feu pour les utilisateurs clients OfficeScan

OfficeScan peut afficher un message de notification sur un ordinateur client immédiatement après que le pare-feu OfficeScan a bloqué du trafic sortant qui viole les

stratégies de pare-feu. Accordez aux utilisateurs le privilège d'activer/désactiver le message de notification.

Remarque

Vous pouvez également activer la notification lorsque vous configurez une stratégie de pare-feu spécifique. Pour configurer une stratégie de pare-feu, voir *Ajout ou modification d'une stratégie de pare-feu à la page 11-11*.

Accorder aux utilisateurs le privilège d'activer/désactiver le message de notification

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges du pare-feu**.
5. Sélectionnez **Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Modification du contenu du message de notification de pare-feu

Tâche

1. Accédez à **Notifications** > **Notifications aux utilisateurs clients**.
2. Cliquez sur l'onglet **Violations du pare-feu**.
3. Saisissez les messages par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de pare-feu

Les journaux de pare-feu disponibles sur le serveur sont envoyés par les clients OfficeScan disposant du privilège d'envoyer des journaux de pare-feu. Accordez à certains clients ce privilège pour surveiller et analyser le trafic sur les ordinateurs clients que le pare-feu OfficeScan bloque.

Pour plus d'informations sur les privilèges du pare-feu, voir *Privilèges du pare-feu à la page 11-24*.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux du pare-feu

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité** ou à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Journaux** > **Journaux de pare-feu** ou sur **Afficher journaux** > **Journaux de pare-feu**.
4. Pour être certain de disposer des journaux les plus à jour, cliquez sur **Demander aux clients**. Patientez jusqu'à ce que les clients aient envoyé les journaux de pare-feu avant de passer à l'étape suivante.
5. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
6. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date et heure de la détection de violation du pare-feu
   - Ordinateur sur lequel la violation du pare-feu s'est produite
   - Domaine de l'ordinateur sur lequel la violation du pare-feu s'est produite
   - Adresse IP de l'hôte distant
   - Adresse IP de l'hôte local
   - Protocole
   - Numéro de port
   - Direction : si le trafic entrant (Recevoir) ou sortant (Envoyer) a violé une stratégie du pare-feu
   - Processus : le programme exécutable ou le service s'exécutant sur l'ordinateur qui a entraîné la violation du pare-feu
   - Description : définit le risque de sécurité effectif (tel qu'un virus de réseau ou une attaque SDI) ou la violation de stratégie de pare-feu

7. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Épidémies de violation du pare-feu

Définissez une épidémie de violations du pare-feu selon le nombre de violations de pare-feu et la période de détection.

OfficeScan est fourni avec un message de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, d'une épidémie. Vous pouvez modifier le message de notification en fonction de vos besoins.

Remarque

OfficeScan peut vous envoyer des notifications d'épidémies du pare-feu par e-mail. Configurez les paramètres de messagerie pour permettre à OfficeScan d'envoyer des e-mails correctement. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 12-32*.

Configuration des critères et notifications de l'épidémie de violation du pare-feu

Tâche

1. Accédez à **Notifications** > **Notifications administrateur** > **Notifications d'épidémies**.
2. Dans l'onglet **Critères** :
   a. Accédez à la section **Violations du pare-feu**.
   b. Sélectionnez **Contrôler les violations du pare-feu sur les ordinateurs en réseau**.
   c. Spécifiez le nombre de journaux SDI, de journaux de pare-feu et de journaux de virus de réseau.

d. Spécifiez la période de détection.

Conseil

Trend Micro recommande d'accepter les valeurs par défaut dans cet écran.

OfficeScan envoie un message de notification lorsque le nombre de journaux est dépassé. Par exemple, si vous spécifiez 100 journaux SDI, 100 journaux de pare-feu et 100 journaux de virus de réseau, ainsi qu'une période de 3 heures, OfficeScan envoie la notification lorsque le serveur reçoit 301 journaux sur une période de 3 heures.

3. Dans l'onglet **Courrier électronique** :

   a. Accédez à la section **Épidémies de violation du pare-feu**.

   b. Sélectionnez **Activer la notification par courrier électronique**.

   c. Indiquez les destinataires de l'e-mail.

   d. Acceptez ou modifiez l'objet et le message par défaut de l'e-mail. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 11-4. Variables de jeton pour les notifications d'épidémie de violation de pare-feu

VARIABLE	DESCRIPTION
%A	Le nombre d'entrées défini pour ce type de journal a été dépassé
%C	Nombre de journaux de violation du pare-feu
%T	Période d'accumulation des journaux de violation du pare-feu

4. Cliquez sur **Enregistrer**.

Test du pare-feu OfficeScan

Pour garantir le bon fonctionnement du pare-feu OfficeScan, effectuez un test sur un client OfficeScan ou le groupe de clients OfficeScan.

AVERTISSEMENT!

Testez les paramètres du client OfficeScan dans un environnement sous contrôle uniquement. N'effectuez aucun test sur des ordinateurs clients connectés au réseau ou à Internet. Cette opération peut exposer les ordinateurs client OfficeScan aux virus, aux attaques pirates, et à d'autres risques.

Tâche

1. Créez et enregistrez une stratégie de test. Configurez les paramètres pour bloquer les types de trafic que vous souhaitez tester. Par exemple, pour empêcher le client OfficeScan d'accéder à Internet, procédez comme suit :
   a. Configurez le niveau de sécurité sur **Faible** (Autoriser tout le trafic entrant/sortant).
   b. Sélectionnez **Activer le pare-feu et Avertir les utilisateurs en cas de violation du pare-feu**.
   c. Créez une exception bloquant le trafic HTTP (ou HTTPS).
2. Créez et enregistrez un profil de test en sélectionnant les clients sur lesquels vous souhaitez tester les fonctions de pare-feu. Associez la stratégie de test au profil de test.
3. Cliquez sur **Affecter un profil aux clients**.
4. Vérifiez le déploiement.
   a. Cliquez sur **Ordinateurs en réseau** > **Gestion des clients**.
   b. Sélectionnez le domaine auquel le client appartient.
   c. Sélectionnez **Affichage pare-feu** dans l'affichage de l'arborescence client.
   d. Vérifiez la présence d'une coche verte dans la colonne **Pare-feu** de l'arborescence des clients. Si vous avez activé le système de détection

d'intrusion pour ce client, vérifiez qu'une coche verte est également présente sous la colonne **SDI**.

e. Vérifiez que le client applique la bonne stratégie de pare-feu. La stratégie apparaît dans la colonne **Stratégie de pare-feu** dans l'arborescence des clients.

5. Testez le pare-feu sur l'ordinateur client en essayant d'envoyer ou de recevoir le type de trafic que vous avez configuré dans la stratégie.

6. Pour tester une stratégie configurée pour empêcher le client d'accéder à Internet, ouvrez un navigateur Web sur l'ordinateur client. Si vous avez configuré OfficeScan pour qu'il affiche un message de notification pour les violations de pare-feu, le message s'affiche sur l'ordinateur client lorsqu'une violation de trafic sortant se produit.

Chapitre 12

Gestion du serveur OfficeScan

Ce chapitre décrit la gestion et les configurations du serveur OfficeScan.

Sujets abordés dans ce chapitre :

- *Administration basée sur les rôles à la page 12-2*
- *Serveurs de référence à la page 12-30*
- *Paramètres de notification aux administrateurs à la page 12-32*
- *Journaux des événements du système à la page 12-35*
- *Gestion du journal à la page 12-36*
- *Sauvegarde de la base de données d'OfficeScan à la page 12-43*
- *Informations relatives au serveur Web OfficeScan à la page 12-45*
- *Mot de passe de la console Web à la page 12-46*
- *Server Tuner à la page 12-48*
- *Smart Feedback à la page 12-51*

Administration basée sur les rôles

Utilisez la fonction d'Administration basée sur les rôles afin d'accorder et de contrôler l'accès à la console Web OfficeScan. Si votre entreprise compte plusieurs administrateurs OfficeScan, vous pouvez utiliser cette fonction pour accorder des privilèges spécifiques de console Web aux administrateurs, et leur proposer uniquement les outils et autorisations nécessaires à la mise en œuvre de ces tâches spécifiques. Vous pouvez également contrôler l'accès à l'arborescence client en leur donnant un ou plusieurs domaines à gérer. De plus, vous pouvez permettre aux non-administrateurs d'avoir un accès en «affichage seulement» à la console Web.

Chaque utilisateur (administrateur ou non) a un rôle spécifique. Un rôle définit le niveau d'accès à la console Web. Les utilisateurs se connectent à la console Web en utilisant des comptes utilisateurs personnalisés ou des comptes Active Directory.

La Role-based administration (administration basée sur les rôles) implique l'exécution des tâches suivantes :

1. Définissez les rôles utilisateurs. Pour obtenir des informations détaillées, voir *Rôles utilisateurs à la page 12-3*.

2. Configurez les comptes utilisateurs et affectez un rôle spécifique à chaque compte utilisateur. Pour obtenir des informations détaillées, voir *Comptes utilisateurs à la page 12-19*.

Affichez les activités de la console Web pour tous les utilisateurs à partir des Journaux des événements du système. Les activités suivantes sont consignées :

- Connexion à la console
- Modification du mot de passe
- Déconnexion de la console
- Expiration de la session (l'utilisateur est automatiquement déconnecté)

Rôles utilisateurs

Le rôle utilisateur détermine les options de menu de la console Web auxquelles un utilisateur peut accéder. Pour chaque option de menu, une autorisation est attribuée au rôle.

Attribuez des autorisations aux éléments suivants :

- *Autorisations de l'option de menu à la page 12-3*
- *Types d'options de menu à la page 12-3*
- *Options de menu pour serveurs et clients à la page 12-4*
- *Options de menu pour les domaines gérés à la page 12-8*
- *Options du menu Gestion des clients à la page 12-9*

Autorisations de l'option de menu

Les autorisations déterminent le niveau d'accès à chaque option de menu. L'autorisation pour une option de menu peut être :

- **Configurer** : autorise l'accès complet à l'option de menu. Les utilisateurs peuvent configurer tous les paramètres, effectuer toutes les tâches, et accéder aux données dans une option de menu.
- **Afficher** : permet aux utilisateurs d'accéder uniquement aux paramètres, tâches et données dans une option de menu.
- **Aucun accès** : permet de masquer une option de menu.

Types d'options de menu

Il existe 3 types d'options de menu dans OfficeScan.

TABLEAU 12-1. Types d'options de menu

TYPE	ÉTENDUE
Options de menu pour les serveurs/clients	• Paramètres, tâches et données du serveur • Données, tâches et paramètres généraux du client Pour obtenir la liste complète des options de menu disponibles, voir *Options de menu pour serveurs et clients à la page 12-4*.
Options de menu pour les domaines gérés	Paramètres, tâches et données détaillés du client, disponibles en dehors de l'arborescence client Pour obtenir la liste complète des options de menu disponibles, voir *Options de menu pour les domaines gérés à la page 12-8*.
Options du menu Gestion des clients	Paramètres, tâches et données détaillés du client, disponibles dans l'arborescence client. Pour obtenir la liste complète des options de menu disponibles, voir *Options du menu Gestion des clients à la page 12-9*.

Options de menu pour serveurs et clients

Le tableau suivant propose une liste des options de menu pour les serveurs/clients :

TABLEAU 12-2. Options de menu pour les serveurs/clients

OPTION DE MENU PRINCIPALE	SOUS-MENUS
Effectuer maintenant un scan de tous les domaines **Remarque** Seuls les utilisateurs disposant d'un rôle administrateur intégré ont accès à cette fonction.	Aucune

OPTION DE MENU PRINCIPALE	SOUS-MENUS

Ordinateurs en réseau	• Gestion des clients
	• Regroupement des clients
	• Paramètres clients généraux
	• Emplacement de l'ordinateur
	• Prévention contre la perte de données
	  • Identificateurs de données
	  • Modèles
	• Vérification de la connexion
	• Prévention des épidémies

Smart Protection	• Sources Smart Protection • Serveur intégré • Smart Feedback

Mises à jour	• Serveur
	  • Mise à jour programmée
	  • Mise à jour manuelle
	  • Source de mise à jour
	• Ordinateurs en réseau
	  • Mise à jour automatique
	  • Source de mise à jour
	• Rétrograder

OPTION DE MENU PRINCIPALE	SOUS-MENUS

Journaux	• Journaux des ordinateurs en réseau
	  • Risques de sécurité
	  • Mise à jour des composants
	• Journaux de mise à jour du serveur
	• Journaux des événements du système
	• Maintenance des journaux

Cisco NAC	• Serveurs Policy Server • Gestion des agents • Déploiement de l'agent • Certificat client

Notifications	• Notifications administrateur
	  • Paramètres généraux
	  • Notifications d’épidémies
	• Notifications aux utilisateurs clients

OPTION DE MENU PRINCIPALE	SOUS-MENUS

Administration	• Comptes utilisateurs
	• Rôles utilisateurs
	
	Remarque
	Seuls les utilisateurs se servant du compte administrateur intégré ont accès aux comptes et rôles utilisateurs.
	• Active Directory
	  • Intégration d'Active Directory
	  • Synchronisation programmée
	• Paramètres proxy
	• Paramètres de connexion
	• Clients inactifs
	• Gestionnaire de quarantaine
	• Licence du produit
	• Paramètres de Control Manager
	• Paramètres de la console Web
	• Sauvegarde de la base de données

Outils	• Outils administrateurs • Outils clients
Plug-in Manager **Remarque** Seuls les utilisateurs se servant du compte administrateur intégré ont accès à cette fonction.	Aucune

Options de menu pour les domaines gérés

Le tableau suivant propose une liste des options de menu pour les domaines gérés :

TABLEAU 12-3. Options de menu pour les domaines gérés

OPTION DE MENU PRINCIPALE	SOUS-MENUS
Résumé **Remarque** Tout utilisateur peut accéder à cette page, quelles que soient les autorisations dont il dispose.	Aucune

Conformité de la sécurité	• Évaluation de conformité
	  • Rapport de conformité
	  • Rapport de conformité planifié
	• Gestion des serveurs externes

Ordinateurs en réseau	• Pare-feu
	  • Stratégies
	  • Profils
	• Installation du client
	  • Basé sur navigateur
	  • Distant

Mises à jour	• Résumé • Ordinateurs en réseau • Mise à jour manuelle

Journaux	• Journaux des ordinateurs en réseau
	  • Vérification de la connexion
	  • Restauration des spywares/ graywares

OPTION DE MENU PRINCIPALE	SOUS-MENUS
Notifications	• Notifications administrateur • Notifications standard

Options du menu Gestion des clients

Le tableau suivant propose une liste des options du menu Gestion des clients :

TABLEAU 12-4. Options du menu Gestion des clients

OPTION DE MENU PRINCIPALE	SOUS-MENUS
État	Aucune
Tâches	• Scan immédiat • Désinstallation du client • Restauration des spywares/graywares

OPTION DE MENU PRINCIPALE	SOUS-MENUS

Paramètres	• Paramètres de scan
	  • Méthodes de scan
	  • Paramètres de scan manuel
	  • Paramètres de scan en temps réel
	  • Paramètres de scan programmé
	  • Paramètres de scan immédiat
	• Paramètres de réputation de sites Web
	• Paramètres de surveillance des comportements
	• Paramètres de contrôle des dispositifs
	• Paramètres de prévention contre la perte de données
	• Paramètres des agents de mise à jour
	• Privilèges et autres paramètres
	• Paramètres des services complémentaires
	• Liste des spywares/graywares approuvés
	• exporter des paramètres
	• importer des paramètres

OPTION DE MENU PRINCIPALE	SOUS-MENUS
Journaux	• Journaux de virus/programmes malveillants • Journaux de spywares/graywares • Journaux de pare-feu • Journaux de réputation de sites Web • Journaux de surveillance des comportements • Journaux de contrôle des dispositifs • Journaux de prévention contre la perte de données • Supprimer des journaux
Gérer l'arborescence des clients	• Ajouter domaine • Renommer domaine • Déplacer client • Trier le client • Supprimer domaine/client
Exporter	Aucune

Rôles utilisateurs intégrés

OfficeScan est fourni avec un ensemble de rôles utilisateurs intégrés que vous ne pouvez ni modifier ni supprimer. Les rôles intégrés sont les suivants :

TABLEAU 12-5. Rôles utilisateurs intégrés

NOM DU RÔLE	DESCRIPTION
Administrateur	Déléguez ce rôle à d'autres administrateurs ou utilisateurs d'OfficeScan ayant une connaissance suffisante d'OfficeScan. Les utilisateurs disposant de ce rôle peuvent configurer toutes les options de menu.

Invité	Déléguez ce rôle aux utilisateurs qui souhaitent afficher la console Web à des fins de référence.
	
	• Les utilisateurs ayant ce rôle n'ont pas accès aux options de menu suivantes :
	  • Effectuer maintenant un scan de tous les domaines
	  • Plug-in Manager
	  • **Administration** > **Rôles utilisateurs**
	  • **Administration** > **Comptes utilisateurs**
	• Les utilisateurs ont un accès en affichage à toutes les autres options du menu.

Trend Power User	Ce rôle est disponible uniquement si vous effectuez une mise à niveau vers OfficeScan 10. Ce rôle hérite des autorisations du rôle « Power User » dans OfficeScan 10. Les utilisateurs disposant de ce rôle peuvent configurer tous les domaines de l'arborescence des clients mais n'ont pas accès aux nouvelles fonctionnalités de cette version.

Rôles personnalisés

Vous pouvez créer des rôles personnalisés si aucun des rôles intégrés ne répond à vos besoins.

Seuls les utilisateurs ayant le rôle d'administrateur intégré et ceux qui utilisent le compte racine créé au cours de l'installation d'OfficeScan peuvent créer des rôles utilisateurs personnalisés et attribuer ces rôles aux comptes utilisateurs.

Ajout d'un rôle personnalisé

Tâche

1. Accédez à **Administration** > **Rôles utilisateurs**.
2. Cliquez sur **Ajouter**. Si le rôle que vous souhaitez créer possède des paramètres semblables à ceux d'un rôle existant, sélectionnez ce dernier et cliquez sur **Copier**. Un nouvel écran s'affiche.
3. Saisissez un nom pour le rôle, ainsi qu'une description facultative.
4. Définissez l'étendue de l'arborescence client.
   a. Cliquez sur **Définir l'étendue de l'arborescence client**. Un nouvel écran s'affiche.
   b. Sélectionnez l'icône du domaine racine ( ). Sinon, vous pouvez choisir un ou plusieurs domaines dans l'arborescence des clients.
   c. Cliquez sur **Enregistrer**.

   Remarque

   Vous ne pourrez pas sauvegarder un rôle personnalisé si vous ne définissez pas l'étendue de l'arborescence client.

   Pour le moment, seuls les domaines ont été définis. La niveau d'accès aux domaines sélectionnés sera défini aux étapes 6 et 7.
5. Cliquez sur l'onglet **Options de menu générales**.
6. Cliquez sur **Options de menu pour les serveurs/clients** et spécifiez l'autorisation pour chaque option de menu disponible. Pour obtenir la liste des options de menu disponibles, voir *Options de menu pour serveurs et clients à la page 12-4*.

   L'étendue de l'arborescence des clients que vous avez configurée à l'étape 3 détermine le niveau d'autorisation afin d'accéder aux options de menu et définit les cibles pour l'autorisation. L'étendue de l'arborescence des clients peut être le domaine racine (tous les clients) ou les domaines spécifiques de l'arborescence des clients.

TABLEAU 12-6. Options de menu pour les serveurs/clients et l'étendue de l'arborescence client

CRITÈRES	ÉTENDUE DE L'ARBORESCENCE CLIENT	
	DOMAINE RACINE	DOMAINES SPÉCIFIQUES
Autorisation de l'option de menu	Configurer, Afficher, ou Aucun accès	Afficher ou Aucun accès
Cible	Le serveur OfficeScan et tous les clients Par exemple, si vous accordez à un rôle la permission de configurer toutes les options de menu pour les serveurs/clients, l'utilisateur peut : • gérer les paramètres, tâches et données du serveur ; • déployer les paramètres clients généraux ; • lancer des tâches client générales ; • gérer des données client générales.	Le serveur OfficeScan et tous les clients Par exemple, si vous accordez à un rôle la permission de configurer toutes les options de menu pour les serveurs/clients, l'utilisateur peut : • Afficher les paramètres, tâches et données du serveur • Afficher les données, tâches et paramètres généraux du client

- Certaines options de menu ne sont pas accessibles aux rôles personnalisés. Par exemple, seuls les utilisateurs ayant le rôle administrateur intégré ont accès au Plug-in Manager, aux rôles utilisateurs et aux comptes utilisateurs.
- Si vous cochez la case sous **Configurer**, la case qui se trouve sous **Afficher** est cochée automatiquement.
- Si vous ne cochez aucune case, l'autorisation est « Aucun accès ».

7. Cliquez sur **Options de menu pour les domaines gérés** et spécifiez l'autorisation pour chaque option de menu disponible. Pour obtenir la liste des options de menu disponibles, voir .

L'étendue de l'arborescence des clients que vous avez configurée à l'étape 3 détermine le niveau d'autorisation afin d'accéder aux options de menu et définit les cibles pour l'autorisation. L'étendue de l'arborescence des clients peut être le domaine racine (tous les clients) ou les domaines spécifiques de l'arborescence des clients.

TABLEAU 12-7. Options de menu pour les domaines gérés et étendue de l'arborescence des clients

CRITÈRES	ÉTENDUE DE L'ARBORESCENCE CLIENT	
	DOMAINE RACINE	DOMAINES SPÉCIFIQUES
Autorisation de l'option de menu	Configurer, Afficher, ou Aucun accès	Configurer, Afficher, ou Aucun accès
Cible	Tous les clients ou certains d'entre eux Exemples : • Si un utilisateur a déployé des stratégie de pare-feu, ces stratégies seront déployées sur tous les clients. • L'utilisateur peut exécuter une mise à jour manuelle du client pour tous les clients ou certains d'entre eux. • Un rapport de conformité peut comporter tous les clients ou certains d'entre eux.	Clients dans les domaines sélectionnés Exemples : • Si un utilisateur a déployé des stratégies de pare-feu, ces stratégies ne seront déployées que sur les clients appartenant aux domaines sélectionnés. • L'utilisateur ne peut exécuter une mise à jour manuelle du client que pour les clients dans les domaines sélectionnés. • Un rapport de conformité ne comprend que les clients appartenant aux domaines sélectionnés.

- Si vous cochez la case sous **Configurer**, la case qui se trouve sous **Afficher** est cochée automatiquement.
- Si vous ne cochez aucune case, l'autorisation est « Aucun accès ».

8. Cliquez sur l'onglet **Options de menu pour les domaines gérés** puis spécifiez l'autorisation pour chaque option de menu disponible. Pour obtenir la liste des options de menu disponibles, voir .

   L'étendue de l'arborescence des clients que vous avez configurée à l'étape 3 détermine le niveau d'autorisation afin d'accéder aux options de menu et définit les cibles pour l'autorisation. L'étendue de l'arborescence des clients peut être le domaine racine (tous les clients) ou les domaines spécifiques de l'arborescence des clients.

TABLEAU 12-8. Options du menu Paramètres clients généraux et étendue de l'arborescence des clients

<table>
<tr><th rowspan="2">CRITÈRES</th><th colspan="2">ÉTENDUE DE L'ARBORESCENCE CLIENT</th></tr>
<tr><th>DOMAINE RACINE</th><th>DOMAINES SPÉCIFIQUES</th></tr>
<tr><td>Autorisation de l'option de menu</td><td>Configurer, Afficher, ou Aucun accès</td><td>Configurer, Afficher, ou Aucun accès</td></tr>
<tr><td rowspan="2">Cible</td><td>Domaine racine (tous les clients) ou domaines spécifiques

Par exemple, vous pouvez accorder à un rôle la permission de configurer l'option de menu « Tâches » dans l'arborescence des clients. Si la cible est le domaine racine, l'utilisateur peut exécuter les tâches pour tous les clients. Si les cibles sont les domaines A et B, les tâches ne peuvent être exécutées que pour les clients des domaines A et B.</td><td>Uniquement les domaines sélectionnés.

Par exemple, vous pouvez accorder à un rôle la permission de configurer l'option de menu « Paramètres » dans l'arborescence des clients. Cela signifie que l'utilisateur peut déployer les paramètres, mais uniquement pour les clients des domaines sélectionnés.</td></tr>
<tr><td colspan="2">L'arborescence des clients ne s'affichera que si l'autorisation pour l'option de menu «Gestion des clients» dans «Options de menu pour les serveurs/clients» est «Afficher».</td></tr>
</table>

- Si vous cochez la case sous **Configurer**, la case qui se trouve sous **Afficher** est cochée automatiquement.
- Si vous ne cochez aucune case, l'autorisation est « Aucun accès ».
- Si vous configurez des autorisations pour un domaine spécifique, vous pouvez copier ces autorisations vers d'autres domaines en cliquant sur **Copier les paramètres du domaine sélectionné vers d'autres domaines**.

9. Cliquez sur **Enregistrer**. Le nouveau rôle s'affiche dans la liste des rôles utilisateurs.

Modification d'un rôle personnalisé

Tâche

1. Accédez à **Administration** > **Rôles utilisateurs**.

2. Cliquez sur le nom du rôle. Un nouvel écran s'affiche.

3. Effectuez les modifications nécessaires sur les éléments suivants :

- Description
- Étendue de l'arborescence client
- Autorisations de rôle
  - Options de menu pour les serveurs/clients
  - Options de menu pour les domaines gérés
  - Options du menu Gestion des clients

4. Cliquez sur **Enregistrer**.

Suppression d'un rôle personnalisé

Tâche

1. Accédez à **Administration** > **Rôles utilisateurs**.

2. Cochez la case qui se trouve à côté du rôle.
3. Cliquez sur **Supprimer**.

Remarque

Un rôle ne peut pas être supprimé s'il est attribué à au moins un compte utilisateur.

Importation ou exportation de rôles personnalisés

Tâche

1. Accédez à **Administration** > **Rôles utilisateurs**.
2. Pour exporter les rôles personnalisés vers un ficher `.dat` :
   a. Sélectionnez les rôles et cliquez sur **Exporter**.
   b. Enregistrez le fichier `.dat`. Si vous gérez un autre serveur OfficeScan, utilisez le fichier `.dat` pour importer des rôles personnalisés dans ce serveur.

Remarque

Seule l'exportation des rôles entres les serveurs disposant d'une version identique est possible.

3. Pour exporter les rôles personnalisés vers un ficher `.csv` :
   a. Sélectionnez les rôles et cliquez sur **Export des paramètres de rôle**.
   b. Enregistrez le fichier `.csv`. Utilisez ce fichier pour vérifier les informations et autorisations des rôles sélectionnés.
4. Si vous avez enregistré des rôles personnalisés à partir d'un serveur OfficeScan différent et si vous souhaitez les importer dans le serveur OfficeScan actuel, cliquez sur **Importer** et recherchez le fichier `.dat` contenant les rôles personnalisés.
   - Dans l'écran Rôles utilisateur, un rôle sera écrasé si vous importez un rôle du même nom.
   - Seule l'importation des rôles entres les serveurs disposant d'une version identique est possible.

- Un rôle importé à partir d'un autre serveur OfficeScan :
  - conserve les autorisations pour les options de menus pour les serveurs/clients et les options de menu pour les domaines gérés ;
  - applique les autorisations par défaut pour les options de menu gestion des clients ; sur l'autre serveur, enregistrez les autorisations du rôle pour les options de menu gestion des clients, puis réattribuez-les au rôle importé.

Comptes utilisateurs

Configurez les comptes utilisateurs et attribuez un rôle particulier à chaque utilisateur. Le rôle de l'utilisateur détermine les options de menu de la console Web qu'un utilisateur peut afficher et configurer.

Au cours de l'installation du serveur OfficeScan, le programme d'installation crée automatiquement un compte intégré nommé «racine». Les utilisateurs qui se connectent en utilisant le compte racine peuvent accéder à toutes les options du menu. Vous ne pouvez pas supprimer le compte racine mais vous pouvez modifier les détails du compte, par exemple le mot de passe et le nom complet ou la description du compte. Si vous oubliez le mot de passe du compte racine, contactez le service d'assistance pour qu'il vous aide à réinitialiser le mot de passe.

Ajoutez des comptes personnalisés ou des comptes Active Directory. Tous les comptes utilisateurs s'affichent dans la liste des comptes utilisateurs de la console Web.

Les comptes utilisateurs d'OfficeScan peuvent être utilisés pour l'«authentification unique». Celle-ci permet aux utilisateurs d'accéder à la console Web d'OfficeScan depuis la console de Trend Micro Control Manager. Pour plus d'informations, consultez la procédure suivante.

Ajout d'un compte personnalisé

Tâche

1. Accédez à **Administration** > **Comptes utilisateurs**.
2. Cliquez sur **Ajouter**.

3. Sélectionnez **Compte personnalisé**.
4. Entrez le nom d'utilisateur, le nom complet et le mot de passe, puis confirmez le mot de passe.
5. Entrez une adresse électronique pour le compte.

Remarque

OfficeScan envoie les notifications à cette adresse e-mail. Les notifications informent le destinataire des risques de sécurité détectés et des transmissions d'actifs numériques. Pour plus de détails sur les notifications, voir *Notifications sur les risques liés à la sécurité pour les administrateurs à la page 6-79* et *Notifications de la prévention contre la perte de données pour les administrateurs à la page 9-56*.

6. Sélectionnez un rôle pour le compte.
7. Cliquez sur **Enregistrer**.
8. Envoyez les détails du compte à l'utilisateur.

Modification d'un compte personnalisé

Tâche

1. Accédez à **Administration** > **Comptes utilisateurs**.
2. Cliquez sur le compte utilisateur.
3. Activez ou désactivez le compte en cliquant sur la case à cocher fournie.
4. Modifiez ce qui suit :
   - Nom complet
   - Mot de passe
   - Adresse électronique
   - Rôle
5. Cliquez sur **Enregistrer**.

6. Envoyez les nouveaux détails du compte à l'utilisateur.

Ajout d'un compte Active Directory ou du groupe

Tâche

1. Accédez à **Administration** > **Comptes utilisateurs**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Utilisateur ou groupe Active Directory**.
4. Indiquez le nom du compte (nom d'utilisateur ou groupe), ainsi que le domaine auquel il appartient.

   Indiquez les noms complets du compte et du domaine. Si les noms de compte et de domaine sont incomplets ou si le groupe par défaut « Utilisateurs du domaine » est utilisé, OfficeScan ne renvoie aucun résultat.

   Tous les membres appartenant à un groupe ont le même rôle. Si un compte particulier appartient à deux groupes au moins et si le rôle des deux groupes est différent :

   - Les autorisations des deux rôles sont fusionnées. Si un utilisateur configure un paramètre particulier et s'il existe un conflit entre des autorisations pour ce paramètre, l'autorisation la plus élevée s'applique.
   - Tous les rôles d'utilisateurs s'affichent dans les journaux d'événements du système. Par exemple, « l'utilisateur John Doe s'est connecté avec les rôles suivants : Administrateur, Invité ».
5. Sélectionnez un rôle pour le compte.
6. Cliquez sur **Enregistrer**.
7. Demandez à l'utilisateur de se connecter à la console Web avec son compte de domaine et son mot de passe.

Ajout de plusieurs comptes Active Directory ou de groupes

Tâche

1. Accédez à **Administration** > **Comptes utilisateurs**.
2. Cliquez sur **Ajouter à partir d'Active Directory**.
3. Recherchez un compte (nom d'utilisateur ou groupe) en indiquant le nom d'utilisateur et le domaine auquel il appartient.

   Remarque

   Utilisez le caractère (*) pour rechercher plusieurs comptes. Si vous n'utilisez pas le caractère générique, indiquez le nom complet du compte. Si les noms de compte sont incomplets ou si le groupe par défaut « Utilisateurs du domaine » est utilisé, OfficeScan ne renvoie aucun résultat.

4. Quand OfficeScan trouve un compte valide, il affiche son nom sous **Utilisateurs et groupes**. Cliquez sur l'icône de transfert (>) pour déplacer le compte sous **Utilisateurs et groupes sélectionnés**.

   Si vous indiquez un groupe Active Directory, tous les membres appartenant à un groupe ont le même rôle. Si un compte particulier appartient à deux groupes au moins et si le rôle des deux groupes est différent :

   - Les autorisations des deux rôles sont fusionnées. Si un utilisateur configure un paramètre particulier et s'il existe un conflit entre des autorisations pour ce paramètre, l'autorisation la plus élevée s'applique.
   - Tous les rôles d'utilisateurs s'affichent dans les journaux d'événements du système. Par exemple, « l'utilisateur John Doe s'est connecté avec les rôles suivants : Administrateur, Power User ».

5. Ajoutez plus de comptes ou de groupes.
6. Sélectionnez un rôle pour les comptes ou les groupes.
7. Cliquez sur **Enregistrer**.

8. Demandez aux utilisateurs de se connecter à la console Web en utilisant leur nom de domaine et leur mot de passe.

Changement d'un rôle de compte personnalisé ou d'un compte Active Directory

Tâche

1. Accédez à **Administration** > **Comptes utilisateurs**.
2. Sélectionnez un ou plusieurs comptes personnalisés ou Active Directory.
3. Cliquez sur **Changer le rôle**.
4. Dans l'écran qui s'affiche, sélectionnez le nouveau rôle, puis cliquez sur **Enregistrer**.

Activation ou désactivation d'un compte personnalisé ou Active Directory

Tâche

1. Accédez à **Administration** > **Comptes utilisateurs**.
2. Cliquez sur l'icône sous **Activer**.

Remarque

Le compte racine ne peut pas être désactivé.

Utilisation des comptes utilisateurs OfficeScan dans Control Manager

Reportez-vous à la documentation de Control Manager pour connaître les étapes détaillées.

Tâche

1. Créez un nouveau compte utilisateur dans Control Manager. Lorsque vous spécifiez le nom d'utilisateur, saisissez le nom du compte qui apparaît sur OfficeScan Web Console.

2. Attribuez au nouveau compte les droits d'« accès » et de « configuration » sur OfficeScan Server.

Remarque

Si un utilisateur de Control Manager a les droits d'« accès » et de « configuration » sur OfficeScan sans avoir de compte OfficeScan, il ne peut accéder à OfficeScan. L'utilisateur voit un message contenant un lien qui ouvre l'écran de connexion d'OfficeScan Web Console.

Trend Micro Control Manager

Trend Micro Control Manager™™ est une console d'administration centralisée qui gère les produits et services Trend Micro au niveau de la passerelle, du serveur de messagerie, du serveur de fichiers et des postes de travail des entreprises. La console d'administration à interface Web de Control Manager fournit un point de surveillance unique pour les produits et services gérés via le réseau.

Control Manager permet aux administrateurs système de surveiller et de notifier les activités telles que les infections, les violations de sécurité ou les points d'entrée de virus. Les administrateurs système peuvent télécharger et déployer des composants dans le réseau, contribuant ainsi à garantir une protection cohérente et à jour. Control Manager autorise les mises à jour à la fois manuelles et programmées, de même que la configuration et la gestion des produits, en groupe ou séparément, afin d'obtenir une flexibilité accrue.

Intégration de Control Manager dans cette version d'OfficeScan

Cette version OfficeScan inclut les fonctionnalités suivantes pour administrer des serveurs OfficeScan à partir de Control Manager :

- Créez, gérez et déployez des stratégies pour l'antivirus OfficeScan, la prévention contre la perte de données ainsi que le contrôle des dispositifs et attribuez directement des privilèges aux clients OfficeScan à partir de la console Control Manager.

  Le tableau suivant énumère les configurations de stratégie disponibles sur Control Manager 6.0.

TABLEAU 12-9. Types de gestion de stratégie OfficeScan sur Control Manager

TYPE DE STRATÉGIE	FONCTIONS
Antivirus et paramètres client OfficeScan	• Paramètres des services complémentaires • Paramètres de surveillance des comportements • Paramètres de contrôle des dispositifs • Paramètres de scan manuel • Privilèges et autres paramètres • Paramètres de scan en temps réel • Liste des spywares/graywares approuvés • Méthodes de scan • Paramètres de scan immédiat • Paramètres de scan programmé • Paramètres des agents de mise à jour • Paramètres de réputation de sites Web
Protection des données	Paramètres de la stratégie de prévention contre la perte de données **Remarque** Gérez les autorisations du contrôle des dispositifs pour la protection des données dans les stratégies client OfficeScan.

- Repliquez les paramètres suivants d'un serveur OfficeScan à un autre à partir de la console Control Manager :

  - *Types d'identificateurs de données à la page 9-13*

- *Modèles de prévention contre la perte de données à la page 9-27*

Remarque

Si ces paramètres sont repliqués vers un serveur OfficeScan sur lequel la licence de protection des données n'a pas bien été activée, les paramètres ne sont pas pris en compte lors de l'activation de la licence.

Versions de Control Manager prises en charge

Cette version d' OfficeScan prend en charge Control Manager 6.0, 5.5 SP1, 5.5 et 5.0.

TABLEAU 12-10. Versions de Control Manager prises en charge

SERVEUR OFFICESCAN	VERSION DE CONTROL MANAGER			
	6.0	5.5 SP1	5.5	5.0
Double pile	Oui	Oui	Oui	Oui
IPv4 pur	Oui	Oui	Oui	Oui
IPv6 pur	Oui	Non	Non	Non

Remarque

L'adressage IPv6 est pris en charge pour Control Manager à partir de la version 5.5 Service Pack 1.

Pour plus d'informations sur les adresses IP faisant l'objet des rapports envoyés par le serveur et les clients OfficeScan à Control Manager, consultez *Écrans affichant les adresses IP à la page A-7*.

Appliquez les patchs les plus récents et les correctifs de type hot fix critiques pour que ces versions de Control Manager permettent à Control Manager de gérer OfficeScan. Pour obtenir les patchs et les correctifs de type hot fix les plus récents, contactez le service d'assistance ou consultez le Centre de mises à jour Trend Micro à l'adresse :

http://www.trendmicro.com/download/emea/?lng=fr

Après avoir installé OfficeScan, enregistrez-le dans Control Manager, puis configurez les paramètres d'OfficeScan dans la console d'administration de Control Manager.

Consultez la *documentation de Control Manager* pour obtenir davantage d'informations sur la gestion des serveurs OfficeScan.

Enregistrement d'OfficeScan sur Control Manager

Tâche

1. Accédez à **Administration** > **Paramètres de Control Manager**.
2. Spécifiez le nom d'affichage de l'entité, qui est le nom du serveur OfficeScan devant s'afficher dans Control Manager.

   Par défaut, le nom d'affichage de l'entité inclut le nom d'hôte de l'ordinateur serveur et le nom de ce produit (par exemple, Server01_OSCE).

   Remarque

   Dans Control Manager, les serveurs OfficeScan et les autres produits gérés par Control Manager sont appelés «entités».

3. Spécifiez le nom de domaine complet ou l'adresse IP du serveur Control Manager et le numéro de port à utiliser pour la connexion à ce serveur. Si vous le souhaitez, vous pouvez optimiser la sécurité de la connexion via HTTPS.

   - Pour un serveur OfficeScan double-pile, saisissez le nom de domaine complet ou l'adresse IP de Control Manager (IPv4 ou IPv6, si disponible).
   - Pour un serveur OfficeScan IPv4, saisissez le nom de domaine complet ou l'adresse IPv4 de Control Manager
   - Pour un serveur OfficeScan IPv6, saisissez le nom de domaine complet ou l'adresse IPv6 de Control Manager

   Remarque

   Seul Control Manager 5.5 SP1 et versions ultérieures prennent en charge IPv6.

4. Si le serveur Web IIS de Control Manager requiert une authentification, saisissez le nom d'utilisateur et le mot de passe.

5. Si vous devez utiliser un serveur proxy pour vous connecter au serveur Control Manager, spécifiez les paramètres proxy suivants :
   - Protocole de serveur proxy
   - Nom de domaine complet ou adresse IPv4/IPv6 et port du serveur
   - ID d'utilisateur et mot de passe d'authentification du serveur proxy
6. Déterminez si vous souhaitez utiliser une redirection de port de communication unilatérale et bilatérale, puis spécifiez les adresses IPv4/IPv6 ainsi que le port.
7. Pour vérifier si OfficeScan peut se connecter au serveur Control Manager avec les paramètres spécifiés, cliquez sur **Tester la connexion**.

   Cliquez sur **Enregistrer** si la connexion a été établie.
8. Après l'enregistrement, si vous modifiez l'un des paramètres sur cet écran, cliquez sur **Paramètres de mise à jour** une fois les paramètres modifiés pour en informer le serveur Control Manager.
9. Si vous ne souhaitez plus que le serveur Control Manager gère OfficeScan, cliquez sur **Annuler l'enregistrement**.

Vérification de l'état d'OfficeScan sur la console d'administration de Control Manager

Tâche

1. Ouvrez la console d'administration de Control Manager.

   Pour ouvrir la console Control Manager, ouvrez un navigateur Web sur un ordinateur quelconque du réseau et entrez l'adresse suivante :

   `https://<nom du serveur Control Manager>/Webapp/login.aspx`

   Dans laquelle `<nom du serveur Control Manager>` correspond à l'adresse IP ou au nom d'hôte du serveur Control Manager.
2. Dans le menu principal, cliquez sur **Produits**.

3. Vérifiez si l'icône du serveur d'OfficeScan s'affiche

Serveurs de référence

L'une des méthodes employées par le client OfficeScan pour déterminer les stratégies ou profils à utiliser consiste à vérifier son état de connexion avec le serveur OfficeScan. Si un client interne OfficeScan (ou un client du réseau d'entreprise) ne peut se connecter au serveur, l'état du client passe à l'état déconnecté. Le client applique ensuite un profil ou une stratégie destinée aux ordinateurs externes. Les serveurs de référence résolvent ce problème.

Un client OfficeScan perdant sa connexion avec le serveur OfficeScan essaiera de se connecter aux serveurs de référence. Si le client parvient à établir une connexion avec le serveur de référence, il applique le profil ou la stratégie aux clients internes.

Les stratégies et profils gérés par les serveurs de référence incluent :

- Profils de pare-feu
- Stratégies de réputation de sites Web
- Stratégies de protection des données
- Stratégies de contrôle des dispositifs

Prenez en compte les éléments suivants :

- Configurez les ordinateurs disposant de capacités de serveur, par exemple des serveurs Web, SQL ou FTP, comme serveurs de référence. Vous pouvez définir au maximum 32 serveurs de référence.
- Les clients OfficeScan se connectent au premier serveur de référence de la liste de serveurs de référence. Si la connexion ne peut pas être établie, le client essaie de se connecter au serveur suivant de la liste.
- Les clients OfficeScan n'utilisent les serveurs de référence que pour déterminer les paramètres relatifs à l'antivirus (surveillance des comportements, contrôle des dispositifs, profils du pare-feu ou stratégie de réputation de sites Web) ou à la protection des données à utiliser. Les serveurs de référence ne gèrent pas les clients

ni ne déploient les mises à jour et les paramètres clients. C'est le serveur OfficeScan qui effectue ces tâches.

- Un client OfficeScan ne peut pas envoyer de journaux à des serveurs de référence ni les utiliser en tant que sources de mise à jour.

Gestion de la liste de serveurs de référence

Tâche

1. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Profils** ou l'**Ordinateurs en réseau** > **Emplacement de l'ordinateur**.
2. En fonction de l'écran qui s'affiche, vous devez procéder de la façon suivante :
   - Si vous vous trouvez dans les pare-feux de profil sur l'écran Ordinateurs en réseau, cliquez sur **Modifier la liste de serveurs de référence**.
   - Si vous êtes sur l'écran Emplacement de l'ordinateur, cliquez sur la **liste de serveurs de référence**.
3. Sélectionnez **Activer la liste de serveurs de référence**.
4. Pour ajouter un ordinateur à la liste, cliquez sur **Ajouter**.
   a. Spécifiez l'adresse IPv4/IPv6 de l'ordinateur, son nom ou son nom de domaine complet (FQDN), par exemple :
      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`
   b. Entrez le numéro de port au moyen duquel les clients communiquent avec cet ordinateur. Spécifiez un port de contact ouvert quelconque (tels que les ports 20, 23 ou 80) sur le serveur de référence.

Remarque

pour spécifier un autre numéro de port pour le même serveur de référence, répétez les étapes 2a et 2b. Le client OfficeScan utilise le premier numéro de port de la liste puis, en cas d'échec de connexion, le numéro de port suivant.

c. Cliquez sur **Enregistrer**.

5. Pour modifier les paramètres d'un ordinateur de la liste, cliquez sur le nom de l'ordinateur. Modifiez le nom ou le port de l'ordinateur puis cliquez sur **Enregistrer**.

6. Pour supprimer un ordinateur de la liste, sélectionnez le nom de l'ordinateur puis cliquez sur **Supprimer**.

7. Pour permettre aux ordinateurs de fonctionner en tant que serveurs de référence, cliquez sur **Attribuer aux clients**.

Paramètres de notification aux administrateurs

Configurez les paramètres de notification aux administrateurs pour permettre à OfficeScan d'envoyer des notifications par e-mail, pageur et déroutement SNMP. OfficeScan peut également envoyer les notifications via le journal des événements Windows NT mais aucun paramètre n'est configuré pour ce canal de notifications.

OfficeSan peut vous envoyer des notifications, ainsi qu'à d'autres administrateurs OfficeScan dans les cas suivants :

TABLEAU 12-11. Détections qui entraînent la notification d'un administrateur

DÉTECTIONS	CANAUX DE NOTIFICATION			
	COURRIER ÉLECTRONIQUE	PAGEUR	DÉROUTEMENT SNMP	JOURNAUX DES ÉVÉNEMENTS WINDOWS NT
Virus et programmes malveillants	Oui	Oui	Oui	Oui

Détections	Canaux de notification			
	Courrier électronique	Pageur	Déroutement SNMP	Journaux des événements Windows NT
Spywares et graywares	Oui	Oui	Oui	Oui
Transmissions des actifs numériques	Oui	Oui	Oui	Oui
Épidémies de virus et de programmes malveillants	Oui	Oui	Oui	Oui
Épidémies de spywares et de graywares	Oui	Oui	Oui	Oui
Épidémies de violation du pare-feu	Oui	Non	Non	Non
Épidémies de sessions de partage de dossiers	Oui	Non	Non	Non

Configuration des paramètres de notifications aux administrateurs

Tâche

1. Accédez à **Notifications** > **Notifications administrateur** > **Paramètres généraux**.
2. Configuration des paramètres de notification par e-mail.
   a. Indiquez une adresse IPv4/IPv6 ou un nom d'ordinateur dans le champ **Serveur SMTP**.
   b. Entrez un numéro de port compris entre 1 et 65535.
   c. Indiquez un nom ou une adresse e-mail.

Si vous voulez activer ESMTP dans la prochaine étape, spécifiez une adresse e-mail valide.

d. Eventuellement, activez **ESMTP**.

e. Spécifiez le nom d'utilisateur et le mot de passe correspondant à l'adresse e-mail que vous avez indiquée dans le champ **De**.

f. Choisissez une méthode pour authentifier le client sur le serveur :

- **Connexion** : la connexion est une ancienne version de l'agent utilisateur mail. Le serveur et le client utilisent tous les deux BASE64 pour authentifier le nom d'utilisateur et le mot de passe.
- Le **Texte brut** est plus simple à utiliser mais peut également être dangereux parce que le nom d'utilisateur et le mot de passe sont envoyés sous forme de chaîne unique et se sont codés en BASE64 avant leur envoi sur Internet.
- **CRAM-MD5**: CRAM-MD5 utilise la combination d'un mécanisme d'authentification par stimulation/réponse et d'un algorithme cryptographique Message Digest 5 pour échanger et authentifier les informations.

3. Configuration des paramètres de notification par pageur.

a. Pour le champ **Pageur**, les caractères suivants sont autorisés :

- de 0 à 9
- #
- *
- ,

b. Entrez un numéro de port COM compris entre 1 et 16.

4. Configuration des paramètres de notification de déroutement SNMP.

a. Indiquez une adresse IPv4/IPv6 ou un nom d'ordinateur dans le champ **Adresse IP du serveur**.

b. Entrez un numéro de communauté difficile à deviner.

5. Cliquez sur **Enregistrer**.

Journaux des événements du système

OfficeScan enregistre les événements liés au programme serveur, tels que les arrêts et les démarrages. Ces journaux permettent de vérifier si le serveur et les services OfficeScan fonctionnent correctement.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 12-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux d'évènements du système

Tâche

1. Accédez à **Journaux** > **Journaux des événements du système**.
2. Sous **Description des événements**, vérifiez les journaux pour lesquels une action supplémentaire est requise. OfficeScan consigne les événements suivants :

TABLEAU 12-12. Journaux des événements du système

TYPE DE JOURNAL	ÉVÉNEMENTS
Service principal d'OfficeScan et serveur de base de données	• Service principal démarré • Service principal fermé correctement • Échec de fermeture du service principal
Prévention des épidémies	• Prévention des épidémies activée • Prévention des épidémies désactivée • Nombre de sessions de partage de dossiers au cours des <nombre de minutes> dernières minutes

TYPE DE JOURNAL	ÉVÉNEMENTS
Sauvegarde de la base de données	• Sauvegarde de la base de données réussie • Sauvegarde de la base de données impossible
Accès à la console Web basé sur les rôles	• Connexion à la console • Modification du mot de passe • Déconnexion de la console • Expiration de la session (l'utilisateur est automatiquement déconnecté)

3. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Gestion du journal

OfficeScan met à votre disposition des journaux complets concernant la détection des risques encourus par la sécurité, les événements, ainsi que les mises à jour. Utilisez ces journaux pour accéder aux stratégies de protection de votre entreprise et pour identifier les clients OfficeScan présentant un risque élevé d'infection ou d'attaque. Ils vous permettent également de vérifier la connexion client-serveur et de vous assurer de la réussite des mises à jour des composants.

OfficeScan utilise également un mécanisme de vérification horaire centralisée pour garantir la cohérence de l'heure entre le serveur OfficeScan et les clients. Cela évite les incohérences entre les journaux provoquées par des différences de fuseau horaire, l'heure d'été et les décalages horaires, qui peuvent engendrer une confusion lors de l'analyse des journaux.

Remarque

OfficeScan effectue la vérification horaire pour tous les journaux excepté les journaux de mise à jour du serveur et les journaux d'événements du système.

Le serveur OfficeScan reçoit les journaux suivants par les clients OfficeScan :

- *Affichage des journaux de virus/programmes malveillants à la page 6-87*
- *Affichage des journaux de spywares/graywares à la page 6-94*
- *Affichage des journaux de restauration de spywares/graywares à la page 6-97*
- *Affichage des journaux du pare-feu à la page 11-31*
- *Affichage de journaux de réputation de sites Web à la page 10-11*
- *Affichage des journaux de surveillance des comportements à la page 7-13*
- *Affichage des journaux de contrôle des dispositifs à la page 8-18*
- *Affichage des journaux de prévention contre la perte de données à la page 9-60*
- *Affichage des journaux de mise à jour du client OfficeScan à la page 5-52*
- *Affichage des journaux de vérification de la connexion à la page 13-45*

Le serveur OfficeScan génère les journaux suivants :

- *Journaux de mise à jour du serveur OfficeScan à la page 5-26*
- *Journaux des événements du système à la page 12-35*

Les journaux suivants sont également disponibles sur le serveur OfficeScan ainsi que les clients OfficeScan :

- *Journaux des événements Windows à la page 17-23*
- *Journaux du serveur OfficeScan à la page 17-3*
- *Journaux du client OfficeScan à la page 17-15*

Maintenance des journaux

Pour éviter que les journaux occupent trop d'espace sur le disque dur, supprimez-les manuellement ou configurez un calendrier de suppression des journaux dans la console Web.

Suppression des journaux sur la base d'une programmation

Tâche

1. Accédez à **Journaux** > **Maintenance des journaux**.
2. Sélectionnez **Activer la suppression programmée des journaux**.
3. Sélectionnez les types de journaux à supprimer. Tous les journaux générés par OfficeScan, à l'exception des journaux de débogage, peuvent être supprimés en fonction d'un planning. Pour les journaux de débogage, désactivez la journalisation de débogage pour interrompre la collecte des journaux.

   Remarque

   Pour les journaux de virus/programmes malveillants, vous pouvez supprimer les journaux générés à partir de certains types de scan et de Damage Cleanup Services. Pour les journaux de spywares/graywares, vous pouvez supprimer les journaux de certains types de scan. Pour plus d'informations concernant les types de scan, voir *Types de scan à la page 6-14*.

4. Spécifiez si les journaux doivent être supprimés pour tous les types de journaux sélectionnés ou uniquement pour les journaux antérieurs à un certain nombre de jours.
5. Spécifiez la fréquence et l'heure de suppression des journaux.
6. Cliquez sur **Enregistrer**.

Suppression manuelle des journaux

Tâche

1. Accédez à **Journaux** > **Journaux des ordinateurs en réseau** > **Risques de sécurité**, ou **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Effectuez l'une des opérations suivantes :

- Si vous accédez à l'écran **Journaux de risques de sécurité pour les ordinateurs en réseau**, cliquez sur **Supprimer des journaux** ou sur **Afficher les journaux** > **Supprimer des journaux**.
- Si vous accédez à l'écran **Paramètres clients généraux**, cliquez sur **Journaux** > **Supprimer les journaux**.

4. Sélectionnez les types de journaux à supprimer. Seuls les journaux suivants peuvent être supprimés manuellement :
   - Journaux de virus/programmes malveillants
   - Journaux de spywares/graywares
   - Journaux de pare-feu
   - Journaux de réputation de sites Web
   - Journaux de contrôle des dispositifs
   - Journaux de surveillance des comportements
   - Journaux de prévention contre la perte de données

Remarque

Pour les journaux de virus/programmes malveillants, vous pouvez supprimer les journaux générés à partir de certains types de scan et de Damage Cleanup Services. Pour les journaux de spywares/graywares, vous pouvez supprimer les journaux de certains types de scan. Pour plus d'informations concernant les types de scan, voir *Types de scan à la page 6-14*.

5. Spécifiez si les journaux doivent être supprimés pour tous les types de journaux sélectionnés ou uniquement pour les journaux antérieurs à un certain nombre de jours.
6. Cliquez sur **Supprimer**.

Licences

Affichez, activez et renouvelez les services de licence OfficeScan sur la console Web et activez/désactivez le pare-feu OfficeScan. La pare-feu OfficeScan fait partie du service antivirus qui inclut également l'assistance pour Cisco NAC et la prévention des épidémies.

Remarque

Certaines fonctionnalités natives d'OfficeScan, telles que la protection des données et Virtual Desktop Support, possèdent leurs propres licences. Les licences pour ces fonctions sont activées et gérées à partir de Plug-in Manager. Pour plus d'informations sur les licences de ces fonctionnalités, consultez *Licence de protection des données à la page 9-4* et *Licence de Virtual Desktop Support à la page 13-79*.

Un serveur IPv6 OfficeScan ne peut pas se connecter au serveur d'enregistrement en ligne Trend Micro pour activer ou renouveler la licence. Un serveur proxy double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur OfficeScan de se connecter au serveur d'enregistrement.

Déconnectez-vous de la console Web, puis reconnectez-vous dans les cas suivants :

- Après avoir activé une licence pour les services de licence suivants :
  - Antivirus
  - Réputation de sites Web et anti-spyware

  Remarque

  La reconnexion est requise pour activer toutes les fonctionnalités du service.

- Après l'activation ou la désactivation du pare-feu OfficeScan. Si vous désactivez le pare-feu, OfficeScan masque toutes les fonctions de pare-feu au niveau du serveur et du client.

Affichage des informations sur la licence produit

Tâche

1. Accédez à **Administration** > **Product License**.

2. Affichez le récapitulatif de l'état des licences, qui apparaît en haut de l'écran. Des messages de rappel concernant les licences s'affichent dans les cas suivants:

   TABLEAU 12-13. Rappels de licence

TYPE DE LICENSE	RAPPEL
Version complète	Pendant la période de grâce du produit. La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro. Une fois la licence expirée et la période de grâce écoulée: pendant cette période, vous ne pourrez ni obtenir d'assistance technique ni effectuer de mises à jour des composants. Les moteurs de scan continueront à scanner les ordinateurs mais utiliseront des composants obsolètes. Ces composants obsolètes ne peuvent pas vous protéger entièrement contre les derniers risques de sécurité.
Version d'évaluation	Une fois la licence expirée: pendant cette période, OfficeScan désactive les mises à jour et le scan des composants, ainsi que toutes les fonctionnalités des clients.

3. Affichez les informations de licence. La section relative aux informations de licence vous fournit les informations suivantes :

   - **Services** : Comprend tous les services de licence d'OfficeScan
   - **État** : affiche « Activé », « Non activé » ou « Expiré ». Si un service dispose de plusieurs licences dont au moins une licence toujours active, l'état « Activé » s'affiche.
   - **Version** : affiche la version « complète » ou la version d'« évaluation ». Si vous disposez à la fois de la version complète et de la version d'évaluation, la version qui s'affiche alors est la version « complète ».

- **Date d'expiration** : Si un service a plusieurs licences, la dernière date d'expiration s'affiche. Par exemple, si les dates d'expiration de la licence sont le 31/12/2007 et le 30/06/2008, la date qui s'affiche est le 30/06/2008.

Remarque

« N/A » correspond aux dates de version et d'expiration des services de licence n'ont pas été activés.

4. OfficeScan vous autorise à activer plusieurs licences pour un service de licence. Cliquez sur le nom du service pour afficher toutes les licences (à la fois actives et expirées) de ce service.

Activation ou renouvellement d'une licence

Tâche

1. Accédez à **Administration** > **Product License**.
2. Cliquez sur le nom du service de licence.
3. Dans l'écran **Détails sur la licence du produit** qui s'ouvre, cliquez sur **Nouveau code d'activation**.
4. Dans l'écran qui s'affiche, saisissez le code d'activation puis cliquez sur **Enregistrer**.

Remarque

Enregistrez un service avant de l'activer. Pour plus d'informations sur la clé d'enregistrement et le code d'activation, contactez votre revendeur Trend Micro.

5. Lorsque vous revenez à l'écran **Détails sur la licence du produit**, cliquez sur **Informations sur la mise à jour** pour actualiser l'écran avec les détails de la nouvelle licence et l'état du service. Cet écran fournit également un lien vers le site Web de Trend Micro sur lequel vous trouverez des informations détaillées relatives à votre licence.

Sauvegarde de la base de données d'OfficeScan

La base de données du serveur OfficeScan contient tous les paramètres OfficeScan, y compris les paramètres de scan et les privilèges. En cas d'altération de la base de données du serveur, vous pouvez la restaurer si vous disposez d'une copie de sauvegarde. Créez une sauvegarde de la base de données manuellement ou configurez un programme de sauvegarde.

Lorsque vous sauvegardez la base de données, OfficeScan vous aide automatiquement à la défragmenter et répare éventuellement toute détérioration du fichier d'index.

Consultez les journaux d'événements du système pour déterminer l'état de la sauvegarde. Pour plus d'informations, voir *Journaux des événements du système à la page 12-35*.

Conseil

Trend Micro recommande de configurer un programme de sauvegarde automatique. Sauvegardez la base de données durant les heures creuses, lorsque le trafic sur le serveur est faible.

AVERTISSEMENT!

N'effectuez pas de sauvegarde avec tout autre outil ou logiciel. Configurez la sauvegarde de la base de données uniquement à partir de la console Web d'OfficeScan.

Sauvegarde de la base de données OfficeScan

Tâche

1. Accédez à **Administration** > **Sauvegarde de la base de données**.
2. Entrez l'emplacement où vous souhaitez enregistrer la base de données. Si le dossier n'existe pas encore, sélectionnez **Créer un dossier s'il n'est pas encore présent**. Précisez le lecteur et le chemin d'accès complet du répertoire, par exemple : `c:\OfficeScan\DatabaseBackup`.

Par défaut, OfficeScan copie la sauvegarde dans le répertoire suivant : <*Dossier d'installation du serveur*>\DBBackup

Remarque

OfficeScan permet de créer un sous-dossier sous le chemin de sauvegarde. Le nom de dossier indique l'heure de la sauvegarde et se présente dans le format suivant : AAAAMMJJ_HHMMSS. OfficeScan conserve les 7 dossiers de sauvegarde les plus récents et supprime le(s) dossier(s) antérieur(s).

3. Si le chemin de sauvegarde désigne un ordinateur distant (en utilisant un chemin UNC), saisissez un nom de compte adapté et le mot de passe correspondant. Vérifiez que le compte dispose des privilèges d'écriture sur l'ordinateur.

4. Pour configurer un programme de sauvegarde :

   a. Sélectionnez **Activer la sauvegarde programmée de la base de données**.

   b. Spécifiez la fréquence et l'heure de sauvegarde.

   c. Pour sauvegarder la base de données et enregistrer les modifications apportées, cliquez sur **Sauvegarder maintenant**. Pour enregistrer sans sauvegarder la base de données, cliquez sur **Enregistrer**.

Restauration des fichiers de sauvegarde de la base de données

Tâche

1. Arrêtez le service principal d'OfficeScan.

2. Remplacez les fichiers de la base de données dans <*Dossier d'installation du serveur*>\PCCSRV\HTTPDB par les fichiers de sauvegarde.

3. Redémarrez le service principal d'OfficeScan.

Informations relatives au serveur Web OfficeScan

Pendant l'installation du serveur OfficeScan, le programme d'installation installe automatiquement un serveur Web (IIS ou serveur Web Apache) qui permet aux ordinateurs en réseau de se connecter au serveur OfficeScan. Configurez le serveur Web auquel les clients des ordinateurs en réseau se connectent.

Si vous modifiez les paramètres de serveur Web de façon externe (par exemple, à partir de la console d'administration IIS), répliquez les modifications dans OfficeScan. Si, par exemple, vous changez manuellement l'adresse IP du serveur pour les ordinateurs en réseau ou si vous lui attribuez une adresse IP dynamique, vous devez reconfigurer les paramètres du serveur OfficeScan.

AVERTISSEMENT!

La modification des paramètres de connexion peut entraîner une perte de connexion permanente entre le serveur et les clients. Vous devrez alors redéployer les clients OfficeScan.

Configuration des paramètres de connexion

Tâche

1. Accédez à **Administration** > **Paramètres de connexion**.
2. Saisissez le nom de domaine ou l'adresse IPv4/IPv6 et le numéro de port du serveur Web.

   Remarque

   Le numéro de port correspond au port sécurisé que le serveur OfficeScan utilise pour communiquer avec les clients OfficeScan.

3. Cliquez sur **Enregistrer**.

Mot de passe de la console Web

L'écran permettant de gérer le mot de passe de la console Web (ou le mot de passe du compte racine créé au cours de l'installation du serveur OfficeScan) n'est accessible que si l'ordinateur serveur ne dispose pas des ressources requises pour utiliser l'administration basée sur les rôles. Par exemple, si l'ordinateur serveur exécute Windows Server 2003 et si Authorization Manager Runtime n'est pas installé, l'écran est accessible. Si les ressources sont adéquates, cet écran ne s'affiche pas et le mot de passe peut être géré en modifiant le compte racine dans l'écran **Comptes utilisateurs**.

Si OfficeScan n'est pas enregistré sur Control Manager, contactez votre service d'assistance pour savoir comment accéder à la console Web.

Paramètres de la console Web

Utilisez l'écran **Paramètres de la console Web** pour :

- Configurez le serveur OfficeScan pour qu'il actualise le tableau de bord récapitulatif de façon périodique. Par défaut, le serveur actualise le tableau de bord toutes les 30 secondes. Le nombre de secondes peut varier entre 10 et 300.
- Définissez les paramètres de délai de la console Web. Par défaut, un utilisateur est automatiquement déconnecté de la console Web après 30 minutes d'inactivité. Le nombre de minutes peut être compris entre 10 et 60.

Configuration des paramètres de la console Web

Tâche

1. Accédez à **Administration** > **Paramètres de la console Web**.
2. Sélectionnez **Activer l'actualisation automatique**, puis sélectionnez l'intervalle d'actualisation.
3. Sélectionnez **Activer la déconnexion automatique de la console Web** , puis sélectionnez l'intervalle de dépassement de délai.

4. Cliquez sur **Enregistrer**.

Gestionnaire de quarantaine

Chaque fois que le client OfficeScan détecte un risque pour la sécurité et que l'action de scan est la mise en quarantaine, il chiffre le fichier infecté, le déplace vers le dossier de quarantaine local situé dans <*Dossier d'installation du client*>>\SUSPECT.

Une fois le fichier déplacé dans le répertoire de quarantaine local, le client OfficeScan l'envoie vers le répertoire de quarantaine désigné. Spécifiez le répertoire dans **Ordinateurs en réseau** > **Paramètres clients généraux > Paramètres** > **{Type de Scan} Paramètres** > **Action**. Les fichiers du répertoire de quarantaine désigné sont chiffrés pour les empêcher d'infecter d'autres fichiers. Voir la *Répertoire de quarantaine à la page 6-40* pour plus d'informations.

Si le répertoire de quarantaine désigné se trouve sur l'ordinateur du serveur OfficeScan, modifiez les paramètres du répertoire de quarantaine du serveur dans la console Web. Le serveur stocke les fichiers mis en quarantaine dans <*Dossier d'installation du serveur*>\PCCSRV\Virus.

Remarque

Si le client OfficeScan ne parvient pas à envoyer le fichier chiffré au serveur OfficeScan pour une raison quelconque, comme un problème de connexion réseau par exemple, le fichier chiffré reste dans le dossier de quarantaine du client. OfficeScan Le client OfficeScan tentera d'envoyer à nouveau le fichier lorsqu'il se connecte au serveur. OfficeScan

Configuration des paramètres du répertoire de quarantaine

Tâche

1. Accédez à **Administration** > **Gestionnaire de quarantaine**.

2. Acceptez ou modifiez la capacité par défaut du dossier de quarantaine et la taille maximum d'un fichier infecté qu'OfficeScan peut stocker dans un dossier de quarantaine.

   Les valeurs par défaut s'affichent à l'écran.

3. Cliquez sur **Enregistrer les paramètres de mise en quarantaine**.

4. Pour supprimer tous les fichiers stockés dans le dossier de quarantaine, cliquez sur **Supprimer tous les fichiers en quarantaine**.

Server Tuner

Utilisez Server Tuner pour optimiser les performances du serveur OfficeScan en utilisant les paramètres pour les questions de performances liées au serveur OfficeScan suivantes :

- **Télécharger**

  Lorsque le nombre de clients OfficeScan (y compris les agents de mise à jour) demandant des mises à jour au serveur OfficeScan excède les ressources disponibles, le serveur place la demande de mise à jour du client dans une file d'attente et traite les demandes lorsque les ressources deviennent à nouveau disponibles. Lorsqu'un client réussit la mise à jour des composants à partir du serveur OfficeScan, il notifie ensuite au serveur la fin de la mise à jour. Définissez le nombre maximum de minutes pendant lesquelles le serveur OfficeScan attend avant de recevoir une notification de mise à jour du client. Définissez aussi le nombre maximum de tentatives de notification du client par le serveur lui demandant d'exécuter une mise à jour et d'appliquer de nouveaux paramètres de configuration. Le serveur essaie uniquement de notifier le client s'il ne reçoit pas automatiquement de notification du client.

- **Buffer**

  Lorsque le serveur OfficeScan reçoit plusieurs demandes des clients OfficeScan, par exemple des demandes de mise à jour, le serveur traite autant de demandes que possible, puis place les autres demandes dans une mémoire tampon. Le serveur traite alors individuellement les demandes enregistrées dans la mémoire tampon au

fur et à mesure que des ressources se libèrent. Précisez la taille de la mémoire tampon pour des événements comme des demandes de mise à jour et de journaux clients.

- **Trafic réseau**

  Le volume de trafic réseau varie pendant la journée. Pour contrôler le flux de trafic réseau vers le serveur OfficeScan et vers les autres sources de mises à jour, précisez le nombre de clients OfficeScan qui peuvent se mettre à jour simultanément à un moment déterminé de la journée.

Serveur Tuner utilise le fichier suivant : `SvrTune.exe`

Exécution du Server Tuner

Tâche

1. Sur l'ordinateur serveur OfficeScan, accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\SvrTune`.
2. Double-cliquez sur le fichier `SvrTune.exe` pour démarrer Server Tuner.

   La console Server Tuner s'ouvre.
3. Sous **Download**, modifiez les données suivantes:

   - **Délai d'attente pour le client** : Saisissez le délai (en nombre de minutes) pendant lequel le serveur OfficeScan attend de recevoir une réponse des clients concernant la mise à jour. Si le client ne répond pas dans ce délai, le serveur OfficeScan considère que le client ne dispose pas des composants actuels. Lorsqu'un client notifié est hors délai, un espace devient disponible pour la notification d'un autre client en attente.
   - **Délai d'attente pour l'agent de mise à jour** : Saisissez le délai (en nombre de minutes) pendant lequel le serveur OfficeScan attend de recevoir une réponse d'un agent de mise à jour concernant la mise à jour. Lorsqu'un client notifié est hors délai, un espace devient disponible pour la notification d'un autre client en attente.

- **Retry count** : Saisissez le nombre maximum de fois que le serveur OfficeScan essaie de notifier un client d'exécuter une mise à jour ou d'appliquer de nouveaux paramètres de configuration.
- **Retry interval** : Saisissez le nombre de minutes d'attente du serveur OfficeScan entre deux tentatives de notification.

4. Sous **Buffer**, modifiez les données suivantes :

   - **Mémoire tampon des événements** : Saisissez le nombre maximum de rapports d'événements clients destinés au serveur (concernant par exemple la mise à jour des composants) conservés par OfficeScan dans la mémoire tampon. La connexion au client est interrompue pendant que la demande du client est en attente dans la mémoire tampon. OfficeScan établit une connexion avec un client lorsqu'il traite le rapport de ce client et le supprime de la mémoire tampon.
   - **Log Buffer** : Saisissez le nombre maximum de rapports de journal d'information clients destinés au serveur et conservées par OfficeScan dans la mémoire tampon. La connexion au client est interrompue pendant que la demande du client est en attente dans la mémoire tampon. OfficeScan établit une connexion avec un client lorsqu'il traite le rapport de ce client et le supprime de la mémoire tampon.

   Remarque

   si un grand nombre de clients communique avec votre serveur, augmentez la taille de la mémoire tampon. Une mémoire tampon de grande taille signifie toutefois une utilisation plus importante de la mémoire du serveur.

5. Sous **Network Traffic**, modifiez les données suivantes :

   - **Heures normales** : Cliquez sur les boutons d'option qui représentent les heures de la journée auxquelles vous considérez que le trafic réseau est normal.
   - **Heures creuses** : Cliquez sur les boutons d'option qui représentent les heures de la journée auxquelles vous considérez que le trafic réseau est à son plus bas niveau.

- **Heures pleines** : Cliquez sur les boutons d'option qui représentent les heures de la journée auxquelles vous considérez que le trafic réseau est à son plus haut niveau.

- **Connexions client maximum** : Saisissez le nombre maximum de clients qui peuvent simultanément mettre à jour des composants, depuis une autre source de mise à jour et depuis le serveur OfficeScan. Saisissez un nombre maximum de clients pour chaque période. Lorsque le nombre maximum de connexions est atteint, un client ne peut mettre à jour des composants qu'après la fermeture d'une connexion client en cours (soit lorsqu'une mise à jour est terminée, soit lorsque le délai de réponse du client dépasse la limite spécifiée dans le champ **Timeout for client** ou **Timeout for Update Agent**).

6. Cliquez sur **OK**. Une invite apparaît vous demandant de relancer le service principal d'OfficeScan.

Remarque

Seul le service redémarre, pas l'ordinateur.

7. Sélectionnez l'une des options de redémarrage suivantes :

   - Cliquez sur **Yes** pour sauvegarder les paramètres de Server Tuner et relancer le service. Les paramètres prennent effet immédiatement après la relance.

   - Cliquez sur **No** pour sauvegarder les paramètres de Server Tuner sans relancer le service. Redémarrez le service principal d'OfficeScan ou redémarrez l'ordinateur du serveur OfficeScan pour que les paramètres soient appliqués.

Smart Feedback

Trend Micro Smart Feedback partage les informations sur les menaces anonymes avec Smart Protection Network, ce qui permet à Trend Micro d'identifier rapidement les nouvelles menaces et d'y répondre. Vous pouvez désactiver Smart Feedback à tout moment via cette console.

Participation au programme Smart Feedback

Tâche

1. Accédez à **Smart Protection** > **Smart Feedback**.
2. Cliquez sur **Activer Trend Micro Smart Feedback**.
3. Pour aider Trend Micro à mieux connaître votre entreprise, sélectionnez son **secteur d'activité**.
4. Pour envoyer des informations sur des menaces de sécurité potentielles figurant dans les fichiers de vos ordinateurs clients, activez la case à cocher **Activer les commentaires sur les fichiers programmes suspects**.

   Remarque

   Les fichiers envoyés à Smart Feedback ne contiennent pas de données utilisateur et ne sont utilisés que pour l'analyse des menaces.

5. Pour configurer les critères d'envoi de vos commentaires, sélectionnez le nombre de détections pour un laps de temps donné qui déclencheront cet envoi.
6. Pour réduire les risques d'interruption du réseau, indiquez la bande passante maximale qu'OfficeScan peut utiliser pour l'envoi des commentaires.
7. Cliquez sur **Enregistrer**.

Chapitre 13

Gestion du client OfficeScan

Ce chapitre décrit la gestion des clients OfficeScan et les configurations de.

Sujets abordés dans ce chapitre :

- *Emplacement de l'ordinateur à la page 13-2*
- *Gestion des programmes du client OfficeScan à la page 13-6*
- *Connexion client-serveur à la page 13-26*
- *Paramètres proxy du client OfficeScan à la page 13-50*
- *Affichage des informations du client OfficeScan à la page 13-55*
- *Importation et exportation des paramètres du client à la page 13-55*
- *Conformité de la sécurité à la page 13-57*
- *Trend Micro Virtual Desktop Support à la page 13-76*
- *Paramètres clients généraux à la page 13-89*
- *Configuration des privilèges clients et autres paramètres à la page 13-90*

Emplacement de l'ordinateur

OfficeScan dispose d'une fonctionnalité de détection d'emplacement qui détermine si l'emplacement d'un client OfficeScan est interne ou externe. La détection d'emplacement est utilisée par les fonctionnalités et services OfficeScan suivants :

TABLEAU 13-1. Fonctionnalités et services utilisant la détection d'emplacement

FONCTIONNALITÉ/ SERVICE	DESCRIPTION
Services de réputation de sites Web	L'emplacement du client OfficeScan détermine la stratégie de réputation de sites Web qui sera appliquée par le client OfficeScan. Les administrateurs appliquent généralement une stratégie plus stricte pour les clients externes. Pour obtenir des informations détaillées sur les stratégies de réputation de sites Web, voir *Stratégies de réputation de sites Web à la page 10-3*.
Services de File Reputation	Pour les clients utilisant Smart Scan, l'emplacement du client OfficeScan détermine la source Smart Protection à laquelle les clients envoient des requêtes de scan. Les clients externes envoient des requêtes de scan à Smart Protection Network alors que les clients internes les envoient aux sources définies dans la liste de sources Smart Protection. Pour plus d'informations concernant les sources Smart Protection, voir *Sources Smart Protection à la page 3-6*.
Prévention contre la perte de données	L'emplacement d'un client OfficeScan détermine la stratégie Prévention contre la perte de données qui sera appliquée par le client. Les administrateurs appliquent généralement une stratégie plus stricte pour les clients externes. Pour plus d'informations sur les stratégies Prévention contre la perte de données, consultez *Stratégies de prévention contre la perte de données à la page 9-11*.

FONCTIONNALITÉ/ SERVICE	DESCRIPTION
Contrôle des dispositifs	L'emplacement d'un client OfficeScan détermine la stratégie de contrôle des dispositifs qui sera appliquée par le client. Les administrateurs appliquent généralement une stratégie plus stricte pour les clients externes. Pour plus d'informations concernant les stratégies de contrôle des dispositifs, voir *Contrôle des dispositifs à la page 8-2*.

Critères d'emplacement

Indiquez si l'emplacement est basé sur l'adresse IP de passerelle de l'ordinateur client OfficeScan ou sur l'état de connexion du client OfficeScan avec le serveur OfficeScan ou un serveur de référence.

- **Adresses IP et MAC de passerelle** : Un ordinateur est considéré comme un ordinateur interne si l'adresse IP de passerelle de l'ordinateur client OfficeScan correspond à l'une des adresses IP de passerelle que vous spécifiez dans l'écran Emplacement de l'ordinateur. Si tel n'est pas le cas, l'emplacement de l'ordinateur est externe.
- **État de la connexion client** : Si le client OfficeScan peut se connecter au serveur OfficeScan ou à l'un des serveurs de référence attribués sur l'intranet, l'emplacement de l'ordinateur est interne. De plus, si un ordinateur hors du réseau de l'entreprise peut se connecter au serveur OfficeScan/serveur de référence, il est également considéré comme un ordinateur interne. Si aucune de ces conditions ne s'applique, l'emplacement de l'ordinateur est externe.

Configuration des paramètres d'emplacement

Tâche

1. Accédez à **Ordinateurs en réseau** > **Emplacement de l'ordinateur**.
2. Indiquez si l'emplacement dépend de l'**état de la connexion client** ou de l'**adresse IP de passerelle et l'adresse MAC**.

3. Si vous choisissez **l'état de la connexion client**, décidez si vous souhaitez utiliser un serveur de référence.

   Voir *Serveurs de référence à la page 12-30* pour obtenir des informations détaillées.

   a. Si aucun serveur de référence n'est spécifié, le client OfficeScan vérifie l'état de connexion avec le serveur OfficeScan lorsque les événements suivants se produisent :

      - Le client OfficeScan passe du mode itinérance au mode normal (en ligne/hors ligne).
      - Le client OfficeScan passe d'une méthode de scan à une autre. Voir *Méthodes de scan à la page 6-8* pour obtenir des informations détaillées.
      - Le client OfficeScan détecte un changement d'adresse IP de l'ordinateur.
      - Le client OfficeScan redémarre.
      - Le serveur lance une vérification de connexion. Voir *Icônes du client OfficeScan à la page 13-26* pour obtenir des informations détaillées.
      - Les critères d'emplacement de la réputation de sites Web changent lors de l'application des paramètres généraux.
      - La stratégie de prévention des épidémies n'est plus appliquée et les paramètres antérieurs à l'épidémie sont restaurés.

   b. Si un serveur de référence est spécifié, le client OfficeScan vérifie d'abord son état de connexion avec le serveur OfficeScan, puis avec le serveur de référence si la connexion au serveur OfficeScan a échoué. Le client OfficeScan vérifie l'état de connexion toutes les heures, ainsi que lorsqu'un des événements ci-dessus se produit.

4. Si vous choisissez **Adresse IP de passerelle et adresse MAC** :

   a. Saisissez l'adresse IPv4/IPv6 de passerelle dans la zone de texte prévue à cet effet.

   b. Saisissez l'adresse MAC.

   c. Cliquez sur **Ajouter**.

Si vous ne saisissez pas d'adresse MAC, OfficeScan inclura toutes les adresses MAC appartenant à l'adresse IP spécifiée.

d. Répétez les étapes a à c jusqu'à ce que toutes les adresses IP de passerelle que vous souhaitez ajouter s'affichent.

e. Utilisez l'outil Gateway Settings Importer pour importer une liste de paramètres de passerelle.

Voir *Gateway Settings Importer à la page 13-5* pour obtenir des informations détaillées.

5. Cliquez sur **Enregistrer**.

Gateway Settings Importer

OfficeScan vérifie l'emplacement d'un ordinateur pour déterminer la stratégie de réputation de sites Web à utiliser et la source Smart Protection auquel il doit se connecter. L'un des procédés employés par OfficeScan pour identifier l'emplacement consiste à vérifier l'adresse IP de passerelle et l'adresse MAC de l'ordinateur.

Configurez les paramètres de passerelle sur l'écran **Emplacement de l'ordinateur** ou utilisez l'outil Outil d'importation de paramètres de passerelle pour importer une liste de paramètres de passerelle vers l'écran **Emplacement de l'ordinateur**.

Utilisation de Gateway Settings Importer

Tâche

1. Préparez un fichier texte (`.txt`) contenant la liste des paramètres de passerelle. Sur chaque ligne, saisissez une adresse IPv4 ou IPv6 et éventuellement une adresse MAC.

   Séparez les adresses IP des adresses MAC par une virgule. Le nombre maximum d'entrées est de 4096.

   Par exemple :

   ```
   10.1.111.222,00:17:31:06:e6:e7
   ```

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334

10.1.111.224,00:17:31:06:e6:e7
```

2. Sur l'ordinateur serveur, accédez à <*Dossier d'installation du serveur*>\PCCSRV\Admin\Utility\GatewaySettingsImporter et double-cliquez sur GSImporter.exe.

Remarque

Vous ne pouvez pas exécuter l'outil Gateway Settings Importer à partir des services Terminal Services.

3. Sur l'écran **Outil d'importation de paramètres de passerelle**, accédez au fichier créé à l'étape 1 et cliquez sur **Importer**.

4. Cliquez sur **OK**.

   Les paramètres de passerelle s'affichent sur l'écran **Emplacement de l'ordinateur** et le serveur OfficeScan déploie les paramètres vers les clients OfficeScan.

5. Pour effacer toutes les entrées, cliquez sur **Effacer tout**.

   Si vous ne devez effacer qu'une entrée particulière, faites-le à partir de l'écran **Emplacement de l'ordinateur**.

6. Pour exporter les paramètres vers un fichier, cliquez sur **Tout exporter**, puis spécifiez le nom et le type du fichier.

Gestion des programmes du client OfficeScan

Les rubriques suivantes traitent des moyens de gérer et de protéger les programmes du client OfficeScan :

- *Services du client OfficeScan à la page 13-7*
- *Redémarrage des services du client OfficeScan à la page 13-12*
- *Autoprotection client à la page 13-13*

- *Sécurité du client OfficeScan à la page 13-17*
- *Restriction de l'accès à la console client OfficeScan à la page 13-18*
- *Déchargement du client OfficeScan à la page 13-19*
- *Privilège des clients OfficeScan itinérants à la page 13-20*
- *Client Mover à la page 13-23*
- *Clients OfficeScan inactifs à la page 13-25*

Services du client OfficeScan

Le client OfficeScan exécute les services répertoriés dans le tableau suivant. Vous pouvez afficher l'état de ces services à partir de Microsoft Management Console.

TABLEAU 13-2. Services du client OfficeScan

SERVICE	FONCTIONNALITÉS CONTRÔLÉES
Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)	• Surveillance des comportements • Contrôle des dispositifs • Certified Safe Software Service • Autoprotection client OfficeScan **Remarque** L'autoprotection client OfficeScan empêche que les services du client OfficeScan ne soient interrompus lorsqu'ils sont activés ou en cours d'exécution.
Pare-feu d'OfficeScan NT (`TmPfw.exe`)	Pare-feu OfficeScan
Service de protection des données OfficeScan (`dsagent.exe`)	• Prévention contre la perte de données • Contrôle des dispositifs

SERVICE	FONCTIONNALITÉS CONTRÔLÉES
Service d'écoute d'OfficeScan NT (`tmlisten.exe`)	Communication entre le client OfficeScan et le serveur OfficeScan
Service proxy d'OfficeScan NT (`TmProxy.exe`)	• Réputation de sites Web • Scan de la messagerie POP3
Service de scan en temps réel d'OfficeScanNT (`ntrtscan.exe`)	• Scan en temps réel • Scan programmé • Scan manuel/Scan immédiat

Les services suivants fournissent une protection solide, mais leurs mécanismes de surveillance peuvent occuper les ressources système, en particulier sur les serveurs exécutant des applications exigeantes en ressources système :

- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)
- Pare-feu d'OfficeScan NT (`TmPfw.exe`)
- Service de protection des données OfficeScan (`dsagent.exe`)

C'est pour cela que ces services sont désactivés par défaut sur les plates-formes serveur (Windows Server 2003 et Windows Server 2008). Si vous souhaitez activer ces services :

- Surveillez constamment les performances du système et effectuez les actions nécessaires lorsque vous remarquez une baisse de performances.
- Pour `TMBMSRV.exe`, vous pouvez activer le service si vous excluez les applications exigeantes en ressources système des stratégies de surveillance des comportements. Vous pouvez utiliser un outil d'optimisation des performances pour identifier les applications exigeantes en ressources système. Pour obtenir des informations détaillées, voir *Utilisation de Trend Micro Performance Tuning Tool à la page 13-10*.

Pour les plates-formes de poste de travail (Windows XP, Vista et 7), ne désactivez les services que si vous remarquez une baisse significative des performances.

Activation ou désactivation des services du client à partir de la console Web

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Pour les clients OfficeScan sur Windows XP, Vista ou 7 :
   a. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

   Remarque

   Après avoir sélectionné le domaine racine ou des domaines spécifiques, le paramètre ne s'appliquera qu'aux clients exécutant Windows XP, Vista ou 7. Le paramètre ne s'appliquera pas aux clients exécutant Windows Server 2003 ou Windows Server 2008, même s'ils font partie des domaines.

   b. Cliquez sur **Paramètres** > **Paramètres des services complémentaires**.
   c. Cochez ou décochez la case dans les sections suivantes :
      - **Service de prévention des modifications non autorisées**
      - **Service de pare-feu**
      - **Service de protection des données**
   d. Cliquez sur **Enregistrer** pour appliquer les paramètres au(x) domaine(s). Si vous avez sélectionné l'icône du domaine racine, choisissez parmi les options suivantes :
      - **Appliquer à tous les clients** : applique les paramètres à tous les clients Windows XP/Vista/7 existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
      - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients Windows XP/Vista/7 ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

3. Pour les clients OfficeScan exécutant Windows Server 2003 ou Windows Server 2008 :

   a. Sélectionnez un client dans l'arborescence client.

   b. Cliquez sur **Paramètres** > **Paramètres des services complémentaires**.

   c. Cochez ou décochez la case dans les sections suivantes :

      - **Service de prévention des modifications non autorisées**
      - **Service de pare-feu**
      - **Service de protection des données**

   d. Cliquez sur **Enregistrer**.

Utilisation de Trend Micro Performance Tuning Tool

Tâche

1. Téléchargez Trend Micro Performance Tuning Tool à partir de :

   http://solutionfile.trendmicro.com/solutionfile/1054312/EN/TMPerfTool_2_90_1131.zip

2. Décompressez `TMPerfTool.zip` pour extraire `TMPerfTool.exe`.

3. Placez `TMPerfTool.exe` dans le <*Dossier d'installation du client*> ou dans le même dossier que `TMBMCLI.dll`.

4. Cliquez avec le bouton droit de la souris sur `TMPerfTool.exe` et sélectionnez **Exécuter en tant qu'administrateur**.

5. Lisez et acceptez le contrat de licence utilisateur final puis cliquez sur **OK**.

6. Cliquez sur **Analyser**.

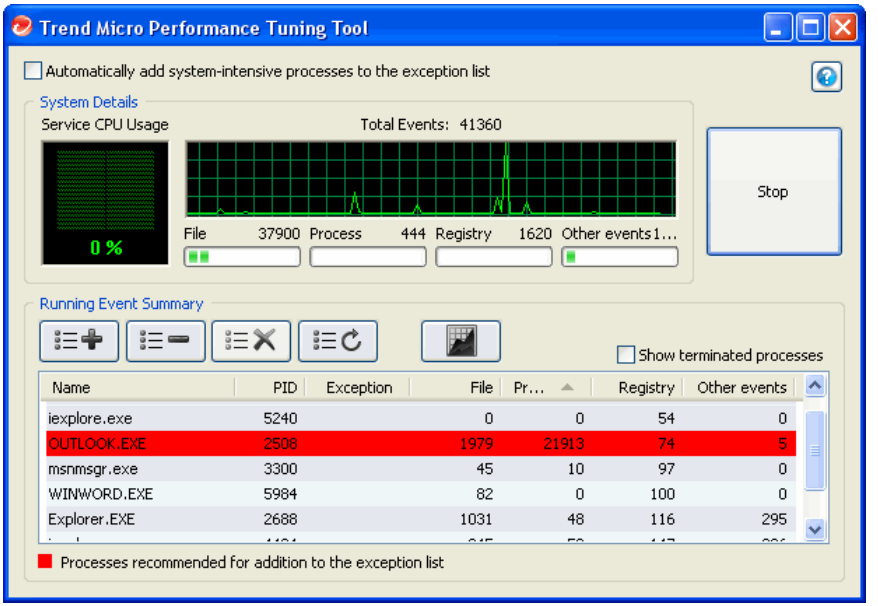

Trend Micro Performance Tuning Tool
Automatically add system-intensive processes to the exception list
System Details
Service CPU Usage
Total Events: 41360
0 %
File 37900 Process 444 Registry 1620 Other events 1...
Stop
Running Event Summary
Show terminated processes
Name PID Exception File Pr... Registry Other events
iexplore.exe 5240 0 0 54 0
OUTLOOK.EXE 2508 1979 21913 74 5
msnmsgr.exe 3300 45 10 97 0
WINWORD.EXE 5984 82 0 100 0
Explorer.EXE 2688 1031 48 116 295
Processes recommended for addition to the exception list

FIGURE 13-1. Processus exigeant en ressources système surligné

L'outil commence à surveiller l'utilisation de l'UC et le chargement d'événements. Un processus exigeant en ressources système est surligné en rouge.

7. Sélectionnez un processus exigeant en ressources système puis cliquez sur le bouton **Ajouter à la liste d'exceptions (autoriser)**.

8. Vérifiez si les performances du système ou des applications s'améliorent.

9. Si elles s'améliorent, sélectionnez à nouveau le processus, puis cliquez sur le bouton **Supprimer de la liste d'exceptions**.

10. Si les performances baissent à nouveau, procédez comme suit :

    a. Notez le nom de l'application.

    b. Cliquez sur **Arrêter**.

    c. Cliquez sur le bouton **Générer le rapport**, puis enregistrez le fichier `.xml`.

d. Vérifiez les applications identifiées comme conflictuelles et ajoutez-les à la liste d'exceptions de surveillance des comportements.

Pour obtenir des informations détaillées, voir *Liste d'exceptions de la surveillance des comportements à la page 7-6*.

Redémarrage des services du client OfficeScan

OfficeScan redémarre les services du client OfficeScan qui ont cessé de répondre de manière inattendue et n'ont pas été arrêtés par un processus système normal. Pour plus d'informations concernant les services du client, voir *Services du client OfficeScan à la page 13-7*.

Configurez les paramètres nécessaires pour permettre aux services du client OfficeScan de redémarrer.

Configuration des paramètres de redémarrage des services

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Allez à la section **Redémarrage d'OfficeScan Service**.
3. Sélectionnez **Redémarrer automatiquement un service de client OfficeScan s'il s'interrompt de façon inattendue**.
4. Configurez les éléments suivants :
   - **Redémarrer le service après ____ minutes** : Indiquez le temps (en minutes) devant s'écouler avant qu'OfficeScan ne redémarre un service.
   - **Si la première tentative de redémarrage du service échoue, réessayer __ fois** : Spécifiez le nombre maximum de nouvelles tentatives pour le redémarrage d'un service. Redémarrez manuellement un service s'il reste arrêté après le nombre maximum de nouvelles tentatives.
   - **Remettre à zéro le compte d'échecs de redémarrage après __ heures** : Si un service reste arrêté une fois que le nombre maximum de nouvelles tentatives a été épuisé, OfficeScan attend un certain nombre d'heures avant de

réinitialiser le compte d'échecs. Si un service reste arrêté une fois que le nombre d'heures est écoulé, OfficeScan le redémarre.

Autoprotection client

L'autoprotection client OfficeScan permet au client OfficeScan de garantir un fonctionnement correct de ses processus et autres ressources nécessaires. L'autoprotection client OfficeScan permet de contrecarrer les tentatives de désactivation de la protection contre les programmes malveillants, qu'elles proviennent de programmes ou d'utilisateurs.

L'autoprotection client OfficeScan fournit les options suivantes :

- *Protéger les services du client OfficeScan à la page 13-14*
- *Protéger les fichiers du dossier d'installation du client OfficeScan à la page 13-15*
- *Protéger les clés de registre du client OfficeScan à la page 13-16*
- *Protéger les processus du client OfficeScan à la page 13-16*

Configuration de l'autoprotection client OfficeScan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) ou sélectionnez des domaines ou des clients spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Autoprotection client**.
5. Activez les options suivantes :
   - *Protéger les services du client OfficeScan à la page 13-14*
   - *Protéger les fichiers du dossier d'installation du client OfficeScan à la page 13-15*
   - *Protéger les clés de registre du client OfficeScan à la page 13-16*

- *Protéger les processus du client OfficeScan à la page 13-16*

Remarque

Par défaut, la protection des clés de registre et des processus est désactivée sur les plates-formes serveur Windows.

6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Protéger les services du client OfficeScan

OfficeScan bloque toutes les tentatives visant à mettre fin aux services du client OfficeScan suivants :

- Service d'écoute d'OfficeScan NT (`TmListen.exe`)
- Service de scan en temps réel d'OfficeScanNT (`NTRtScan.exe`)
- Service proxy d'OfficeScan NT (`TmProxy.exe`)
- Pare-feu d'OfficeScan NT (`TmPfw.exe`)
- Service de protection des données OfficeScan (`dsagent.exe`)
- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)

Remarque

Si cette option est activée, OfficeScan peut empêcher l'installation de produits tiers sur les points finaux. Si vous rencontrez ce problème, vous pouvez désactiver temporairement l'option, puis la réactiver une fois le produit tiers installé.

Protéger les fichiers du dossier d'installation du client OfficeScan

Pour empêcher les autres programmes ou l'utilisateur de modifier ou de supprimer les fichiers du client OfficeScan, OfficeScan verrouille les fichiers suivants dans le <*dossier d'installation du client*> racine :

- Tous les fichiers signés numériquement possédant les extensions `.exe`, `.dll` et `.sys`
- Certains fichiers sans signature numérique, dont :
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`

- patchw64.dll
- PiReg.exe
- ssleay32.dll
- Tmeng.dll
- TMNotify.dll
- zlibwapi.dll

Protéger les clés de registre du client OfficeScan

OfficeScan bloque toutes les tentatives de modification, suppression ou ajout de nouvelles entrées sous les clés et sous-clés de registre suivantes :

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMCSS

Protéger les processus du client OfficeScan

OfficeScan bloque toutes les tentatives visant à mettre fin aux processus suivants :

- TmListen.exe: Reçoit des commandes et notifications depuis le serveur OfficeScan et facilite la communication entre le client OfficeScan et le serveur.
- NTRtScan.exe: Effectue des scans en temps réel, programmés et manuels sur les clients OfficeScan
- TmProxy.exe: Scanne le trafic réseau avant que celui-ci ne puisse atteindre l'application cible
- TmPfw.exe: Offre des fonctions de pare-feu au niveau paquet, de recherche de virus de réseau et de détection d'intrusion
- TMBMSRV.exe: Régule l'accès aux périphériques de stockage externes et empêche la modification non autorisée des clés de registre et des processus

- `DSAgent.exe`: Surveille la transmission de données sensibles et contrôle l'accès aux périphériques

Sécurité du client OfficeScan

Contrôlez l'accès des utilisateurs aux paramètres du registre et du répertoire d'installation du client OfficeScan en sélectionnant l'un des deux paramètres de sécurité.

Contrôle de l'accès au répertoire d'installation et aux clés de registre client OfficeScan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) ou sélectionnez des domaines ou des clients spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Paramètres de sécurité du client**.
5. Sélectionnez l'une des autorisations d'accès suivantes :
   - **Élevé** : Le répertoire d'installation client OfficeScan hérite des droits du dossier `Program Files` et les entrées de registre client OfficeScan héritent des autorisations de la clé `HKLM\Software`. Pour la plupart des configurations d'Active Directory, les utilisateurs "normaux" (qui ne disposent pas de privilèges d'administrateur) sont dès lors limités à un accès en lecture seule.
   - **Normal** : Cette autorisation donne à tous les utilisateurs (le groupe d'utilisateurs « Tous ») les pleins droits sur le répertoire du programme client OfficeScan et les entrées de registre client OfficeScan.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Restriction de l'accès à la console client OfficeScan

Ce paramètre désactive l'accès à la console client OfficeScan depuis la barre d'état système ou le menu Démarrer de Windows. Les utilisateurs ne peuvent alors accéder à la console client OfficeScan qu'en cliquant sur `PccNT.exe` dans le <*dossier d'installation du client*>. Après avoir configuré ce paramètre, rechargez le client OfficeScan pour qu'il entre en vigueur.

Ce paramètre ne désactive pas le client OfficeScan. Le client OfficeScan s'exécute en arrière-plan et continue d'assurer une protection contre les risques de sécurité.

Restriction de l'accès à la console client OfficeScan

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) ou sélectionnez des domaines ou des clients spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Accès restreint à la console client**.
5. Sélectionnez **Ne pas autoriser les utilisateurs à accéder à la console client depuis la barre d'état système ou le menu Démarrer de Windows**.

6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Déchargement du client OfficeScan

Le privilège de déchargement du client OfficeScan autorise les utilisateurs à arrêter momentanément le client OfficeScan avec ou sans mot de passe.

Accord de privilège de déchargement du client

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) ou sélectionnez des domaines ou des clients spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Déchargement**.
5. Pour autoriser le déchargement d'un client sans mot de passe, sélectionnez **Autoriser l'utilisateur à décharger le client OfficeScan**.
   - SI un mot de passe est nécessaire, sélectionnez **Demander un mot de passe à l'utilisateur lors du déchargement du client OfficeScan**, entrez le mot de passe et confirmez-le.

6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Privilège des clients OfficeScan itinérants

Accordez à certains utilisateurs le privilège des clients OfficeScan itinérants si les événements client-serveur interfèrent avec les tâches des utilisateurs. Par exemple, un utilisateur qui donne fréquemment des présentations peut activer le mode itinérance avant de lancer une présentation pour empêcher le serveur OfficeScan de déployer les paramètres du client OfficeScan et de lancer un scan sur le client OfficeScan.

Lorsque les clients sont en mode itinérance :

- Les clients OfficeScan n'envoient pas de journaux au serveur OfficeScan, même si la connexion entre le serveur et les clients est opérationnelle.
- Le serveur OfficeScan n'initie pas de tâches et ne déploie pas de paramètres clients OfficeScan pour les clients, même si la connexion entre le serveur et les clients est opérationnelle.
- Les clients OfficeScan mettent à jour les composants s'ils peuvent se connecter à l'une de leurs sources de mises à jour. Ces sources peuvent être le serveur OfficeScan, des agents de mise à jour ou une source de mise à jour personnalisée.

  Les événements suivants déclenchent une mise à jour pour les clients itinérants :

  - L'utilisateur effectue une mise à jour manuelle.
  - La mise à jour automatique du client s'exécute. Vous pouvez désactiver la mise à jour automatique du client pour les clients itinérants. Pour obtenir des

informations détaillées, voir *Désactivation de la mise à jour automatique du client pour les clients itinérants à la page 13-22*.

- Une mise à jour programmée s'exécute. Seuls les clients disposant des privilèges nécessaires peuvent exécuter des mises à jour programmées. Vous pouvez retirer ce privilège à tout moment. Pour obtenir des informations détaillées, voir *Retrait du privilège de mise à jour programmée aux clients OfficeScan itinérants à la page 13-22*.

Accord de privilège de mode itinérance du client

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) ou sélectionnez des domaines ou des clients spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilège de mode itinérance**.
5. Sélectionnez **Activer le mode itinérance**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Désactivation de la mise à jour automatique du client pour les clients itinérants

Tâche

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**.
2. Allez à la section **Mise à jour déclenchée par un événement**.
3. Désactivez **Inclure le(s) client(s) itinérant(s) et hors ligne**.

> **Remarque**
>
> Cette option est automatiquement désactivée lorsque vous désactivez **Lancer la mise à jour des composants sur les clients immédiatement après le téléchargement d'un nouveau composant sur le serveur OfficeScan**.

4. Cliquez sur **Enregistrer**.

Retrait du privilège de mise à jour programmée aux clients OfficeScan itinérants

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) ou sélectionnez des domaines ou des clients spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de mise à jour des composants**.
5. Désactivez l'option **Activer la mise à jour programmée**.
6. Cliquez sur **Enregistrer**.

Client Mover

Si vous disposez de plusieurs serveurs OfficeScan sur le réseau, utilisez l'outil Client Mover pour transférer des clients OfficeScan d'un serveur OfficeScan vers un autre. Cet outil est particulièrement utile lorsque vous ajoutez un nouveau serveur OfficeScan au réseau, pour transférer des clients OfficeScan existants vers ce nouveau serveur.

Remarque

Les deux serveurs doivent posséder une version dans la même langue. Si vous utilisez Client Mover pour déplacer un client OfficeScan qui exécute une version antérieure sur un serveur utilisant la version actuelle, le client OfficeScan sera mis à niveau automatiquement.

Assurez-vous que le compte que vous utilisez a des privilèges d'administrateur avant d'utiliser cet outil.

Exécution de Client Mover

Tâche

1. Sur le serveur OfficeScan, accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Copiez `IpXfer.exe` sur l'ordinateur du client OfficeScan. Si l'ordinateur client OfficeScan exécute une plate-forme x64, copiez `IpXfer_x64.exe`.
3. Sur l'ordinateur client OfficeScan, ouvrez une invite de commande et accédez au dossier dans lequel vous avez copié le fichier exécutable.
4. Exécutez Client Mover à l'aide de la syntaxe suivante :

```
<nom du fichier exécutable> -s <nom du serveur> -p <port d'écoute du serveur> -c <port d'écoute client> -d <domaine ou hiérarchie de domaines>
```

TABLEAU 13-3. Paramètres de Client Mover

PARAMÈTRE	EXPLICATION
`<nom de fichier exécutable>`	`IpXfer.exe` OU `IpXfer_x64.exe`

PARAMÈTRE	EXPLICATION
`<nom du serveur>`	Nom du serveur OfficeScan de destination (serveur vers lequel le client OfficeScan doit être transféré)
`<port d'écoute du serveur>`	Port d'écoute (ou Port sécurisé) du serveur OfficeScan de destination. Pour afficher le port d'écoute sur la console Web d'OfficeScan, cliquez sur **Administration** > **Paramètres de connexion** dans le menu principal.
`<port d'écoute client>`	Numéro de port utilisé par l'ordinateur client OfficeScan pour communiquer avec le serveur.
`<domaine ou hiérarchie des domaines>`	Domaine ou sous-domaine de l'arborescence des clients dans lequel le client sera regroupé. La hiérarchie des domaines doit indiquer le sous-domaine.

Exemples :

```
ipXfer.exe -s Serveur01 -p 8080 -c 21112 -d Groupe de
travail
```

```
ipXfer_x64.exe -s Serveur02 -p 8080 -c 21112 -d Groupe de
travail\Groupe01
```

5. Pour vérifier que le client OfficeScan dépend maintenant de l'autre serveur, procédez comme suit :

   a. Sur l'ordinateur client OfficeScan, cliquez avec le bouton droit de la souris sur l'icône du programme client OfficeScan dans la barre d'état système.

   b. Sélectionnez la **console OfficeScan**.

   c. Cliquez sur **Aide** dans le menu et sélectionnez **À propos de**.

   d. Vérifiez de quel serveur OfficeScan le client OfficeScan dépend dans le champ **Nom du serveur/port**.

Remarque

Si le client OfficeScan ne s'affiche pas dans l'arborescence des clients du nouveau serveur OfficeScan qui prendra en charge sa gestion, redémarrez le Service principal du nouveau serveur (`ofservice.exe`).

Clients OfficeScan inactifs

Lorsque vous utilisez le programme de désinstallation du client OfficeScan pour supprimer le client OfficeScan sur un ordinateur, le programme en informe automatiquement le serveur. Dès qu'il reçoit cette information, le serveur supprime l'icône du client OfficeScan dans l'arborescence des clients, indiquant ainsi que le client n'existe plus.

En revanche, si vous utilisez d'autres méthodes pour désinstaller le client OfficeScan, comme le reformatage du disque dur de l'ordinateur ou la suppression manuelle des fichiers du client OfficeScan, OfficeScan n'est pas informé de cette suppression et considère le client OfficeScan comme un client inactif. Lorsqu'un utilisateur décharge ou désactive le client OfficeScan sur une longue période, le serveur considère également le client OfficeScan comme étant inactif.

Pour que l'arborescence des clients affiche uniquement les clients actifs, configurez OfficeScan de telle sorte qu'il supprime automatiquement de l'arborescence tous les clients inactifs.

Suppression automatique des clients inactifs

Tâche

1. Accédez à **Administration** > **Clients inactifs**.
2. Sélectionnez **Activer la suppression automatique des clients inactifs**.
3. Précisez ensuite combien de jours doivent s'écouler avant qu'OfficeScan considère un client OfficeScan comme étant inactif.
4. Cliquez sur **Enregistrer**.

Connexion client-serveur

Le client OfficeScan doit maintenir une connexion continue avec son serveur parent afin de pouvoir mettre à jour les composants, recevoir des notifications et appliquer des modifications à la configuration en temps et en heure. Les rubriques suivantes traitent des méthodes permettant de vérifier l'état de connexion du client OfficeScan et de résoudre les problèmes de connexion :

- *Adresses IP du client à la page 4-8*
- *Icônes du client OfficeScan à la page 13-26*
- *Vérification de la connexion client-serveur à la page 13-43*
- *Journaux de vérification de la connexion à la page 13-44*
- *Clients inaccessibles à la page 13-45*

Icônes du client OfficeScan

L'icône du client OfficeScan dans la barre d'état système fournit des conseils visuels qui indiquent l'état actuel du client et invitent les utilisateurs à effectuer certaines actions. À un moment donné, l'icône présentera une combinaison des conseils visuels suivants.

TABLEAU 13-4. État du client OfficeScan indiqué dans l'icône de client OfficeScan

ÉTAT DU CLIENT	DESCRIPTION	CONSEIL VISUEL
Connexion du client au serveur OfficeScan	Les clients en ligne sont connectés au serveur OfficeScan. Le serveur peut initier des tâches et déployer les paramètres vers ces clients.	L'icône contient un symbole représentant un battement de cœur. La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel.
	Les clients hors ligne sont déconnectés du serveur OfficeScan. Le serveur ne peut pas gérer ces clients.	L'icône contient un symbole représentant l'arrêt d'un battement de cœur. La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel. Un client a la possibilité de passer en mode hors ligne même s'il est connecté au réseau. Pour obtenir des informations sur ce problème, voir *Un client OfficeScan est connecté au réseau mais apparaît hors ligne à la page 13-41*.
	Les clients itinérants sont soit capables de communiquer avec le serveur OfficeScan, soit incapables de communiquer avec celui-ci.	L'icône contient les symboles de bureau et de signal. La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel. Pour plus d'informations sur les clients itinérants, voir *Privilège des clients OfficeScan itinérants à la page 13-20*.

ÉTAT DU CLIENT	DESCRIPTION	CONSEIL VISUEL
Disponibilité des sources Smart Protection	Les sources Smart Protection incluent les serveurs Smart Protection Server et Trend Micro Smart Protection Network. Les clients de scan traditionnel se connectent aux sources Smart Protection pour les requêtes de réputation de sites Web. Les clients Smart Scan se connectent aux sources Smart Protection pour les requêtes de scan et de réputation de sites Web.	L'icône contient une coche si une source Smart Protection est disponible.
		L'icône contient une barre de progression si aucune source Smart Protection n'est disponible et que le client tente d'établir la connexion avec les sources. Pour obtenir des informations sur ce problème, voir *Les sources Smart Protection ne sont pas disponibles à la page 13-42*.
		Pour les clients de scan traditionnel, aucune coche ni barre de progression ne s'affiche si la réputation de sites Web a été désactivée.

ÉTAT DU CLIENT	DESCRIPTION	CONSEIL VISUEL
État du service de scan en temps réel	OfficeScan utilise le service de scan en temps réel non seulement pour le scan en temps réel mais également pour les scans manuel et programmé. Le service doit être opérationnel ou le client devient vulnérable aux risques de sécurité.	Toute l'icône est ombrée en bleu si le service de scan en temps réel fonctionne. Deux nuances de bleu sont utilisées pour indiquer la méthode de scan du client. • Pour le scan traditionnel : • Pour Smart Scan :
		Un ombrage rouge est appliqué à l'intégralité de l'icône si le service de scan en temps réel a été désactivé ou ne fonctionne pas. Deux nuances de rouge sont utilisées pour indiquer la méthode de scan du client. • Pour le scan traditionnel : • Pour Smart Scan : Pour obtenir des informations sur ce problème, voir *Le service de scan en temps réel a été désactivé ou ne fonctionne pas à la page 13-41*.

ÉTAT DU CLIENT	DESCRIPTION	CONSEIL VISUEL
État du scan en temps réel	Le scan en temps réel fournit une protection proactive en scannant les fichiers au moment où ils sont créés, modifiés ou récupérés, afin de détecter tout risque de sécurité.	Il n'y a pas de conseils visuels si le scan en temps réel est activé.
		Toute l'icône est entourée d'un cercle rouge et contient une ligne diagonale rouge si le scan en temps réel est désactivé. Pour obtenir des informations sur ce problème, voir : • *Scan en temps réel désactivé à la page 13-41* • *Scan en temps réel désactivé et client OfficeScan en mode itinérant à la page 13-41*
État de mise à jour du fichier de signatures	Les clients doivent mettre à jour régulièrement le fichier de signatures pour protéger le client contre les nouvelles menaces.	Il n'y a aucun conseil visuel si le fichier de signatures est à jour ou légèrement obsolète.
		L'icône contient un point d'exclamation si le fichier de signatures est largement obsolète. Cela signifie que le fichier de signatures n'a pas été mis à jour depuis longtemps. Pour plus d'informations sur les modalités de mise à jour des clients, consultez *Mise à jour des clients OfficeScan à la page 5-27*.

Icônes Smart Scan

Les icônes suivantes peuvent s'afficher lorsque les clients OfficeScan utilisent Smart Scan.

TABLEAU 13-5. Icônes Smart Scan

ICÔNE	CONNEXION AVEC LE SERVEUR OFFICESCAN	DISPONIBILITÉ DES SOURCES SMART PROTECTION	SERVICE DE SCAN EN TEMPS RÉEL	SCAN EN TEMPS RÉEL
	En ligne	Disponible	Opérationnel	Activé
	En ligne	Disponible	Opérationnel	Désactivé
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Hors ligne	Disponible	Opérationnel	Activé
	Hors ligne	Disponible	Opérationnel	Désactivé
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé

Icône	Connexion avec le serveur OfficeScan	Disponibilité des sources Smart Protection	Service de scan en temps réel	Scan en temps réel
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Itinérant	Disponible	Opérationnel	Activé
	Itinérant	Disponible	Opérationnel	Désactivé
	Itinérant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Activé
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	Itinérant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel

Icônes de scan traditionnel

Les icônes suivantes peuvent s'afficher lorsque les clients OfficeScan utilisent le scan traditionnel.

TABLEAU 13-6. Icônes de scan traditionnel

ICÔNE	CONNEXION AVEC LE SERVEUR OFFICESCAN	SERVICES DE RÉPUTATION DE SITES WEB FOURNIS PAR LES SOURCES SMART PROTECTION	SERVICE DE SCAN EN TEMPS RÉEL	SCAN EN TEMPS RÉEL	FICHIER DE SIGNATURES DE VIRUS
	En ligne	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	En ligne	Disponible	Opérationnel	Activé	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète
	En ligne	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Disponible	Opérationnel	Désactivé	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Disponible	Opérationnel	Activé	Largement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète
	Hors ligne	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Disponible	Opérationnel	Désactivé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Itinérant	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	Itinérant	Disponible	Opérationnel	Activé	Largement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Itinérant	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Itinérant	Disponible	Opérationnel	Désactivé	Largement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	Itinérant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Itinérant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	En ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Activé	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Activé	Largement obsolète
	En ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Désactivé	Largement obsolète
	En ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	En ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Activé	Largement obsolète
	Hors ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Désactivé	Largement obsolète
	Hors ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Itinérant	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Activé	À jour ou légèrement obsolète
	Itinérant	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Activé	Largement obsolète
	Itinérant	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Itinérant	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Opérationnel	Désactivé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Itinérant	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Itinérant	Sans objet (fonction de réputation de sites Web désactivée pour le client)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète

Solutions à des problèmes indiqués par les icônes de clients OfficeScan

Exécutez les actions nécessaires lorsque l'icône du client OfficeScan signale l'une des situations suivantes :

Le fichier de signatures n'a pas été mis à jour depuis un certain temps

Les utilisateurs clients OfficeScan doivent mettre à jour les composants. Depuis la console Web, vous pouvez configurer les paramètres de mise à jour des composants dans **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique**, ou accorder aux utilisateurs le privilège de mise à jour dans **Ordinateurs en réseau** > **Gestion des clients** > **Paramètres** > **Privilèges et autres paramètres** > **Privilèges** > **Privilèges de mise à jour des composants**.

Le service de scan en temps réel a été désactivé ou ne fonctionne pas

Si le service de scan en temps réel (OfficeScan NT RealTime Scan) a été désactivé ou ne fonctionne plus, les utilisateurs doivent démarrer le service manuellement à partir de Microsoft Management Console.

Scan en temps réel désactivé

Activez le scan en temps réel depuis la console Web (**Ordinateurs en réseau** > **Gestion des clients > Paramètres** > **Paramètres de scan** > **Paramètres de scan en temps réel**).

Scan en temps réel désactivé et client OfficeScan en mode itinérant

Les utilisateurs doivent d'abord désactiver le mode itinérance. Après la désactivation du mode itinérance, activez le scan en temps réel depuis la console Web.

Un client OfficeScan est connecté au réseau mais apparaît hors ligne

Vérifiez la connexion depuis la console Web (**Ordinateurs en réseau** > **Vérification de la connexion**), puis examinez les journaux de vérification de la connexion (**Journaux** > **Journaux des ordinateurs en réseau** > **Vérification de la connexion**).

Si le client OfficeScan est toujours hors ligne après la vérification :

1. Si l'état de la connexion est hors ligne à la fois sur le serveur et sur le client OfficeScan, vérifiez la connexion réseau.

2. Si l'état de la connexion est hors ligne sur le client OfficeScan et en ligne sur le serveur, le nom de domaine du serveur peut avoir été modifié et le client OfficeScan se connecte au serveur à l'aide du nom de domaine (si vous avez sélectionné le nom de domaine au cours de l'installation du serveur). Enregistrez le nom de domaine du serveur OfficeScan sur le serveur DNS ou WINS, ou ajoutez le nom de domaine et les données IP dans le fichier « hosts » du dossier `<dossier Windows>\system32\drivers\etc` de l'ordinateur client.

3. Si l'état de la connexion sur le client OfficeScan est en ligne alors qu'il est hors ligne sur le serveur, vérifiez les paramètres de pare-feu OfficeScan. Le pare-feu risque de bloquer la communication serveur-client, mais autorise la communication client-serveur.

4. Si l'état de la connexion sur le client OfficeScan est en ligne alors qu'il est hors ligne sur le serveur, l'adresse IP du client OfficeScan peut avoir été modifiée, mais son état n'apparaît pas sur le serveur (par exemple, lorsque le client est rechargé). Essayez de redéployer le client OfficeScan.

Les sources Smart Protection ne sont pas disponibles

Effectuez ces tâches si un client perd la connexion avec les sources Smart Protection :

1. Sur la console Web, accédez à l'écran Emplacement de l'ordinateur (**Ordinateurs en réseau** > **Emplacement de l'ordinateur**) et vérifiez si les paramètres d'emplacement d'ordinateur ont été configurés correctement :
   - Serveurs de référence et numéros de port
   - Adresses IP de passerelle
2. Sur la console Web, accédez à l'écran Source Smart Protection (**Smart Protection** > **Sources Smart Protection**), puis procédez comme suit :
   a. Vérifiez si les paramètres du serveur Smart Protection Server dans la liste standard ou personnalisée des sources sont corrects.
   b. Vérifiez si la connexion aux serveurs peut être établie.
   c. Cliquez sur **Notifier tous les clients** après avoir configuré la liste des sources.
3. Vérifiez si les fichiers suivants du serveur Smart Protection Server et du client OfficeScan sont synchronisés :
   - `sscfg.ini`
   - `ssnotify.ini`
4. Ouvrez l'éditeur du registre et vérifiez si un client est connecté au réseau d'entreprise.

   Clé :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
   \CurrentVersion\iCRC Scan\Scan Server
   ```

- Si `LocationProfile=1`, le client OfficeScan est connecté au réseau et doit pouvoir se connecter à Smart Protection Server.
- Si `LocationProfile=2`, le client OfficeScan n'est pas connecté au réseau et doit pouvoir se connecter à Smart Protection Network. Dans Internet Explorer, vérifiez si l'ordinateur client OfficeScan peut naviguer sur les pages Web.

5. Vérifiez les paramètres proxy internes et externes utilisés pour la connexion à Smart Protection Network et aux serveurs Smart Protection Server. Pour obtenir des informations détaillées, voir *Proxy interne pour les clients OfficeScan à la page 13-50* et *Proxy externe pour les clients OfficeScan à la page 13-51*.

6. Pour les clients de scan traditionnel, assurez-vous que le service proxy NT d'OfficeScan (`TmProxy.exe`) est en cours d'exécution. Si ce service s'arrête, les clients ne peuvent pas se connecter aux sources Smart Protection pour la réputation de sites Web.

Vérification de la connexion client-serveur

L'état de la connexion client au serveur OfficeScan s'affiche dans l'arborescence des clients d'OfficeScan Web Console.

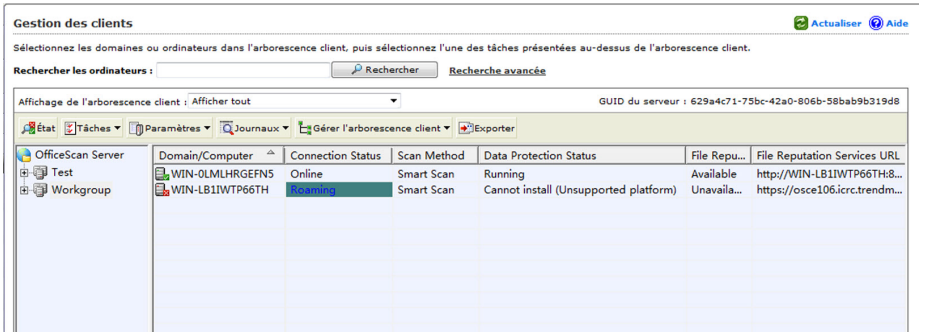


FIGURE 13-2. Arborescence des clients affichant l'état de la connexion client au serveur OfficeScan

Dans certains cas, l'affichage de l'état correct de la connexion du client dans l'arborescence des clients est impossible. Par exemple, si vous débranchez

accidentellement le câble réseau d'un ordinateur client, le client ne pourra pas informer le serveur qu'il est déconnecté. Dans l'arborescence des clients, le client apparaîtra toujours comme étant connecté.

Vérifiez la connexion client-serveur manuellement ou laissez OfficeScan effectuer la vérification programmée. Vous ne pouvez pas sélectionner des domaines ou clients spécifiques, puis vérifier leur état de connexion. OfficeScan contrôle l'état de la connexion de tous ses clients enregistrés.

Vérification de la connexion serveur-client

Tâche

1. Accédez à **Ordinateurs en réseau** > **Vérification de la connexion**.
2. Pour vérifier manuellement la connexion client-serveur, accédez à l'onglet **Vérification manuelle** et cliquez sur **Vérifier maintenant**.
3. Pour vérifier manuellement la connexion client-serveur, cliquez sur l'onglet **Vérification programmée**.
   a. Sélectionnez **Activer la vérification programmée**.
   b. Sélectionnez la fréquence et l'heure de début de la vérification.
   c. Cliquez sur **Enregistrer** pour enregistrer la programmation de vérification établie.
4. Vérifiez l'arborescence des clients pour contrôler l'état ou consulter les journaux de vérification de la connexion.

Journaux de vérification de la connexion

OfficeScan conserve les journaux de vérification de connexion pour vous permettre de déterminer si oui ou non le serveur OfficeScan peut communiquer avec l'ensemble de ses clients enregistrés OfficeScan crée une entrée de journal chaque fois que vous vérifiez la connexion serveur-client à partir de la console Web.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du*

journal à la page 12-36 pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de vérification de la connexion

Tâche

1. Accédez à **Ordinateurs en réseau** > **Vérification de la connexion**.
2. Consultez le résultat de vérification de la connexion en vérifiant la colonne **État**.
3. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Clients inaccessibles

Des clients OfficeScan sur des réseaux inaccessibles, comme ceux qui se trouvent sur des segments du réseau derrière une passerelle NAT, sont presque toujours hors ligne car le serveur ne peut pas établir une connexion directe avec ces clients. Par conséquent, le serveur ne peut pas demander à ces clients de :

- Télécharger des derniers composants.
- Appliquer les paramètres du client configurés sur la console web. Par exemple, lorsque vous changez la fréquence du scan programmé sur la console Web, le serveur avertit immédiatement les clients d'appliquer le nouveau paramètre.

Par conséquent, les clients inaccessibles ne peuvent pas effectuer ces tâches en temps et en heure. Ils n'effectuent ces tâches que lorsqu'ils établissent la connexion avec le serveur, ce qui se produit lorsque :

- Ils s'enregistrent sur le serveur après l'installation.
- Ils redémarrent ou se rechargent. Cet événement ne se produit pas fréquemment et nécessite généralement l'intervention de l'utilisateur.
- Une mise à jour manuelle ou programmée est déclenchée sur le client. Cet événement ne se produit pas fréquemment non plus.

Le serveur n'est informé de la connectivité des clients et ne les traite comme étant en ligne que lors de l'enregistrement, du redémarrage ou du rechargement. Toutefois, du fait que le serveur n'est toujours pas en mesure d'établir la connexion avec les clients, il change immédiatement leur état pour les traiter comme étant hors ligne.

OfficeScan offre les fonctions «battement de cœur» et d'interrogation du serveur pour résoudre les problèmes concernant les clients inaccessibles. Avec ces fonctions, le serveur cesse de notifier les clients des mises à jour de composants et des changements de paramètres. À la place, le serveur prend un rôle passif, attendant toujours que les clients envoient le battement de cœur ou lancent l'interrogation. Lorsque le serveur détecte n'importe lequel de ces événements, il traite les clients comme étant en ligne.

Remarque

Les événements initiés par le client qui ne sont pas associés au battement de cœur ou à l'interrogation du serveur, par exemple la mise à jour manuelle du client et l'envoi de journaux, ne déclenchent pas la mise à jour par le serveur de l'état inaccessible des clients.

Battement de cœur

Des clients OfficeScan envoient des messages de pulsation pour prévenir le serveur que la connexion à partir du client reste fonctionnelle. Lorsqu'il reçoit un message de battement de cœur, le serveur traite le client comme étant en ligne. Dans l'arborescence client, l'état du client peut être :

- **En ligne** : Pour les clients ordinaires en ligne
- **Inaccessible/en ligne** : Pour les clients en ligne sur le réseau inaccessible

Remarque

Les clients OfficeScan ne mettent pas à jour les composants et n'appliquent pas les nouveaux paramètres lors de l'envoi de messages de pulsation. Les clients ordinaires réalisent ces opérations durant les mises à jour courantes (voir *Mise à jour des clients OfficeScan à la page 5-27*). Les clients du réseau inaccessible effectuent ces tâches au cours de l'interrogation du serveur.

La fonction de pulsation résout le problème des clients OfficeScan sur des réseaux inaccessibles et apparaissant toujours comme étant hors ligne bien qu'ils puissent se connecter au serveur.

Un paramètre de la console Web contrôle la fréquence à laquelle les clients envoient des messages de battement de cœur. Si le serveur n'a pas reçu de battement de cœur, il ne traite pas immédiatement le client comme étant hors ligne. Un autre paramètre contrôle la durée sans battement de cœur devant s'écouler avant de changer l'état du client en :

- **Hors ligne** : Pour les clients OfficeScan ordinaires hors ligne
- **Inaccessible/hors ligne** : Pour les clients OfficeScan hors ligne sur le réseau inaccessible

Lorsque vous choisissez une configuration de battements de cœur, il s'agit de trouver le juste équilibre entre la nécessité d'afficher les dernières informations d'état du client et celle de gérer les ressources système. Le paramètre par défaut est satisfaisant dans la plupart des situations. Cependant, tenez compte des points suivants lorsque vous personnalisez la configuration des battements de cœur :

TABLEAU 13-7. Recommandations relatives aux battements de cœur

FRÉQUENCE DU BATTEMENT DE CŒUR	RECOMMANDATION
Battements de cœur à intervalles longs (plus de 60 minutes)	Plus l'intervalle entre les battements de cœur est long, plus le nombre d'événements pouvant se produire avant que l'état du client ne soit indiqué sur la console Web du serveur est élevé.
Battements de cœur à intervalles courts (moins de 60 minutes)	Les intervalles courts présentent un état du client mieux actualisé mais peuvent consommer beaucoup de bande passante.

Interrogation du serveur

La fonctionnalité d'interrogation du serveur résout le problème des clients OfficeScan inaccessibles qui ne reçoivent pas les notifications en temps et en heure concernant les mises à jour de composants et les changements des paramètres du client. Cette fonction est indépendante de la fonction battement de cœur.

Avec la fonction d'interrogation du serveur :

- Les clients OfficeScan établissent automatiquement la connexion au serveur OfficeScan à intervalles réguliers. Lorsque le serveur détecte l'interrogation, il traite les clients comme étant «Inaccessibles/en ligne».

- Les clients OfficeScan se connectent à une ou plusieurs de leurs sources de mise à jour pour télécharger les éventuels composants mis à jour et appliquer les nouveaux paramètres du client. Si le serveur OfficeScan ou un agent de mise à jour est la source de mise à jour principale, les clients obtiennent à la fois les composants et les nouveaux paramètres. Si la source n'est pas le serveur OfficeScan ou un agent de mise à jour, les clients obtiennent seulement les composants mis à jour, puis se connectent au serveur OfficeScan ou à l'agent de mise à jour pour obtenir les nouveaux paramètres.

Configuration des fonctions de battement de cœur et d'interrogation du serveur

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Allez sur la section **Réseau inaccessible**.
3. Configurez les paramètres de l'interrogation du serveur.

   Pour plus de détails sur l'interrogation du serveur, voir *Interrogation du serveur à la page 13-47*.

   a. Si le serveur OfficeScan possède à la fois une adresse IPv4 et IPv6, vous pouvez saisir une plage d'adresses IPv4 ainsi qu'un préfixe et une longueur IPv6.

      Saisissez une plage d'adresses IPv4 si le serveur est en IPv4 pur ou un préfixe et une longueur IPv6 si le serveur est en IPv6 pur.

      Lorsque l'adresse IP d'un client correspond à l'une des adresses de la plage, le client applique les paramètres de battement de cœur et d'interrogation du serveur et ce dernier traite le client comme faisant partie d'un réseau inaccessible.

Remarque

Des clients ayant une adresse IPv4 ne peuvent pas se connecter à un pure IPv4 ou à un serveur OfficeScan à double pile .

Des clients ayant une adresse IPv6 peuvent se connecter à un pure IPv6 ou à un serveur OfficeScan à double pile.

Des clients Dual-stack peuvent se connecter à un serveur OfficeScan à double pile, pure IPv4, ou pure IPv6.

b. Dans **Les clients interrogent le serveur pour obtenir les composants et paramètres mis à jour toutes les __ minute(s)**, indiquez la fréquence d'interrogation du serveur. Saisissez une valeur comprise entre 1 et 129600 minutes.

Conseil

Trend Micro recommande que la fréquence d'interrogation du serveur représente au moins trois fois la fréquence d'envoi du battement de cœur.

4. Configurez les paramètres de battement de cœur.

Pour plus d'informations sur la fonction battement de cœur, voir *Battement de cœur à la page 13-46*.

a. Sélectionnez **Autoriser les clients à envoyer le battement de cœur au serveur**.

b. Sélectionnez **Tous les clients** ou **Uniquement les clients sur le réseau inaccessible**.

c. Dans **Les clients envoient le battement de cœur toutes les __ minutes**, indiquez la fréquence à laquelle les clients envoient un battement de cœur. Saisissez une valeur comprise entre 1 et 129600 minutes.

d. Dans **Un client est hors ligne en l'absence d'un battement de cœur au bout de __ minutes**, indiquez la durée sans battement de cœur devant s'écouler avant que le serveur OfficeScan considère le client comme étant hors ligne. Saisissez une valeur comprise entre 1 et 129600 minutes.

5. Cliquez sur **Enregistrer**.

Paramètres proxy du client OfficeScan

Configurez les clients OfficeScan pour qu'ils utilisent des paramètres proxy lors de la connexion aux serveurs internes et externes.

Proxy interne pour les clients OfficeScan

Les clients OfficeScan peuvent utiliser les paramètres de proxy internes pour se connecter aux serveurs suivants du réseau :

- **Ordinateur du serveur OfficeScan**

  L'ordinateur serveur héberge le serveur OfficeScan et le serveur Smart Protection Server intégré. Les clients OfficeScan se connectent au serveur OfficeScan afin de mettre à jour des composants, d'obtenir des paramètres de configuration, et envoyer des journaux. les clients OfficeScan se connectent au serveur intégré Smart Protection Server afin d'envoyer des requêtes de scan.

- **serveurs Smart Protection Server**

  Les serveurs Smart Protection Server comprennent tous les serveurs Smart Protection Server autonomes et les serveurs Smart Protection Server intégrés des autres serveurs OfficeScan. Les clients OfficeScan se connectent aux serveurs pour envoyer des requêtes de scan et de réputation de sites Web.

Configuration des paramètres proxy internes

Tâche

1. Accédez à **Administration** > **Paramètres proxy**.
2. Cliquez sur l'onglet **Proxy interne**.
3. Allez à la section **Connexion du client à l'ordinateur du serveur OfficeScan**.

a. Sélectionnez **Utilisez les paramètres proxy suivants lorsque les clients se connectent au serveur OfficeScan et au serveur Smart Protection Server intégré.**.

b. Indiquez le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.

Remarque

Indiquez un serveur proxy double pile identifié par son nom d'hôte si vous avez des clients IPv4 et IPv6. Ceci est dû au fait que les paramètres de proxy interne sont des paramètres globaux. Si vous indiquez une adresse IPv4, les clients Pv6 ne peuvent se connecter au serveur proxy. Il s'agit de la même chose pour les clients IPv4.

c. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

4. Allez à la section **Connexion des clients aux serveurs Smart Protection Server autonomes**.

   a. Sélectionnez **Utilisez les paramètres proxy suivants lorsque les clients se connectent aux serveurs Smart Protection Server autonomes**.

   b. Indiquez le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.

   c. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

5. Cliquez sur **Enregistrer**.

Proxy externe pour les clients OfficeScan

Le serveur OfficeScan et le client OfficeScan peuvent utiliser des paramètres proxy externe lorsqu'ils se connectent à des serveurs hébergés par Trend Micro. Cette rubrique présente les paramètres de proxy externe pour les clients. Pour connaître les paramètres de proxy externe pour le serveur, voir *Proxy pour les mises à jour du serveur OfficeScan à la page 5-18*.

Les clients OfficeScan utilisent les paramètres de proxy configurés dans Internet Explorer pour se connecter à Trend Micro Smart Protection Network. Si une authentification sur le serveur proxy est nécessaire, les clients utiliseront les informations d'authentification du serveur proxy (ID utilisateur et mot de passe).

Configuration des informations d'authentification sur le serveur proxy

Tâche

1. Accédez à **Administration** > **Paramètres proxy**.
2. Cliquez sur l'onglet **Proxy externe**.
3. Allez à la section **Connexion du client aux serveurs Trend Micro**.
4. Saisissez l'ID utilisateur et le mot de passe nécessaires à l'authentification du serveur proxy, puis confirmez le mot de passe. Les protocoles d'authentification sur le serveur proxy suivants sont pris en charge :
   - Authentification d'accès de base
   - Authentification d'accès Digest
   - Authentification intégrée de Windows
5. Cliquez sur **Enregistrer**.

Privilèges de configuration proxy pour les clients

Vous pouvez accorder aux utilisateurs clients l'autorisation de configurer les paramètres proxy. Les clients OfficeScan n'utilisent les paramètres proxy configurés par l'utilisateur que dans les cas suivants :

- Lorsque les clients OfficeScan exécutent l'option « Mettre à jour ».
- Lorsque les paramètres proxy automatiques sont désactivés par les utilisateurs ou que le client OfficeScan ne parvient pas à les détecter. Voir la*Paramètres proxy automatique pour le client OfficeScan à la page 13-53* pour plus d'informations.

AVERTISSEMENT!

Des paramètres proxy configurés par l'utilisateur incorrects peuvent entraîner des problèmes de mise à jour. Soyez prudent lorsque vous autorisez les utilisateurs à configurer leurs propres paramètres proxy.

Attribution de privilèges de configuration proxy

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section Privilèges de paramètres proxy.
5. Sélectionnez **Autoriser l'utilisateur client à configurer des paramètres proxy**.
6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Paramètres proxy automatique pour le client OfficeScan

La configuration manuelle des paramètres proxy peut s'avérer complexe pour la plupart des utilisateurs finaux. Utilisez la configuration automatique des paramètres proxy pour

garantir l'application de paramètres proxy corrects sans que l'intervention de l'utilisateur soit requise.

Lorsqu'ils sont activés, les paramètres proxy automatiques sont prioritaires lorsque les clients OfficeScan mettent à jour les composants au moyen de la mise à jour automatique ou de l'option Update Now. Voir *Méthodes de mise à jour du client OfficeScan à la page 5-37* pour obtenir des informations complémentaires sur la mise à jour automatique et sur l'option Mettre à jour.

Si les clients OfficeScan ne peuvent pas se connecter à l'aide des paramètres proxy automatiques, les utilisateurs clients bénéficiant du privilège de configuration des paramètres proxy peuvent procéder eux-mêmes à la configuration de ces paramètres. Sinon, la connexion à l'aide des paramètres proxy automatiques échoue.

Remarque

L'authentification du serveur proxy n'est pas prise en charge.

Configuration des paramètres proxy automatiques

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Allez dans la section **Configuration proxy**.
3. Sélectionnez **Détecter automatiquement les paramètres** si vous souhaitez qu'OfficeScan détecte automatiquement les paramètres proxy configurés par l'administrateur par DHCP ou DNS.
4. Si vous souhaitez qu'OfficeScan utilise le script de configuration proxy automatique (PAC, pour « proxy auto-configuration ») défini par l'administrateur réseau pour détecter le serveur proxy approprié :
   a. Sélectionnez **Utiliser le script de configuration automatique**.
   b. Tapez l'adresse du script PAC.
5. Cliquez sur **Enregistrer**.

Affichage des informations du client OfficeScan

L'écran Afficher l'état affiche d'importantes informations relatives aux clients OfficeScan, notamment les privilèges, les informations détaillées sur le logiciel client et les événements système.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **État**.
4. Affichez les informations relatives à l'état en développant le nom de l'ordinateur client. Si vous avez sélectionné plusieurs clients, cliquez sur **Développer tout** pour afficher les informations relatives à l'état pour tous les clients sélectionnés.
5. (Facultatif) Utilisez le bouton **Réinitialiser** pour remettre à zéro le décompte de risques de sécurité.

Importation et exportation des paramètres du client

OfficeScan vous permet d'exporter les paramètres de l'arborescence client appliqués à un fichier par un client OfficeScan ou un domaine particulier. Vous pouvez ensuite importer le fichier afin d'appliquer les paramètres à d'autres clients et domaines, ou à un autre serveur OfficeScan d'une version identique.

Tous les paramètres de l'arborescence des clients, à l'exception des paramètres de l'agent de mise à jour, seront exportés.

Exportation des paramètres du client

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Exporter paramètres**.
4. Cliquez sur un des liens pour afficher les paramètres du client OfficeScan ou du domaine sélectionné.
5. Cliquez sur **Exporter** pour enregistrer les paramètres.

   Les paramètres sont enregistrés dans un fichier `.dat`.
6. Cliquez sur **Enregistrer**, puis indiquez dans quel dossier le fichier `.dat` doit être enregistré.
7. Cliquez sur **Enregistrer**.

Importation des paramètres du client

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Importer des paramètres**.
4. Cliquez sur **Parcourir** pour localiser le fichier `.dat` sur l'ordinateur, puis cliquez sur **Importer**.

   L'écran **Importer les paramètres** apparaît ; il affiche un résumé des paramètres.
5. Cliquez sur un des liens pour afficher les informations concernant les paramètres de scan ou les privilèges à importer.

6. Procédez à l'importation des paramètres.

   - Si vous avez cliqué sur l'icône du domaine racine, sélectionnez **Appliquer à tous les domaines**, puis cliquez sur **Appliquer à la cible**.
   - Si vous avez sélectionné des domaines, sélectionnez **Appliquer à tous les ordinateurs appartenant au(x) domaine(s) sélectionné(s)**, puis cliquez sur **Appliquer à la cible**.
   - Si vous avez sélectionné plusieurs clients, cliquez sur **Appliquer à la cible**.

Conformité de la sécurité

Utilisez la conformité de la sécurité pour déterminer les failles, déployer des solutions et gérer l'infrastructure de sécurité. Cette fonctionnalité aide les administrateurs à réduire le temps requis pour sécuriser l'environnement réseau et permet d'équilibrer les besoins de l'entreprise en termes de sécurité et de fonctionnalité.

Appliquez la conformité de la sécurité pour deux types d'ordinateurs :

- **Gérés** : Ordinateurs avec des clients OfficeScan gérés par le serveur OfficeScan. Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les clients gérés à la page 13-58*.
- **Non gérés** : Comprend les éléments suivants :
  - Clients OfficeScan non gérés par le serveur OfficeScan
  - Ordinateurs sans clients OfficeScan installés
  - Ordinateurs que le serveur OfficeScan ne peut atteindre
  - Ordinateurs dont l'état de sécurité ne peut être vérifié

    Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les points finaux non gérés à la page 13-71*.

Conformité de la sécurité pour les clients gérés

La conformité de la sécurité génère un rapport Conformité pour vous aider à évaluer l'état de sécurité des clients OfficeScan gérés par le serveur OfficeScan. La conformité de la sécurité génère le rapport à la demande ou en fonction d'une programmation.

Les rapports à la demande et programmés sont disponibles sur l'écran Rapport de conformité. L'écran contient les onglets suivants :

- **Services** : utilisez cet onglet pour vérifier si les services clients sont opérationnels. Pour obtenir des informations détaillées, voir *Services à la page 13-59*.
- **Composants** : utilisez cet onglet pour vérifier si les composants des clients OfficeScan sont à jour. Pour obtenir des informations détaillées, voir *Composants à la page 13-61*.
- **Conformité du scan** : utilisez cet onglet pour vérifier si les clients OfficeScan effectuent régulièrement des scans. Pour obtenir des informations détaillées, voir *Conformité du scan à la page 13-63*.
- **Paramètres**: utilisez cet onglet pour vérifier si les paramètres clients sont cohérents avec les paramètres du serveur. Pour obtenir des informations détaillées, voir *Paramètres à la page 13-64*.

Remarque

L'onglet **Composants** peut afficher les clients OfficeScan utilisant la dernière version et les versions antérieures du produit. Pour les autres onglets, seuls les clients OfficeScan utilisant la version 10.5, 10.6 ou une version supérieure sont affichés.

Notes sur le rapport de conformité

- La conformité de la sécurité interroge l'état de connexion des clients OfficeScan avant de générer un rapport Conformité. Les clients en ligne et hors ligne sont compris dans le rapport, mais pas les clients itinérants.
- Pour les comptes utilisateurs basés sur les rôles :
  - Chaque compte utilisateur de la console Web possède un ensemble de paramètres de rapport de conformité totalement indépendant. Aucun

changement dans les paramètres de rapport de conformité d'un compte utilisateur n'affectera les paramètres des autres comptes utilisateurs.

- L'étendue du rapport dépend des autorisations sur les domaines clients des comptes utilisateurs. Par exemple, si vous accordez à un compte utilisateur les autorisations de gérer les domaine A et B, les rapports du compte utilisateur n'afficheront que les données des clients appartenant aux domaines A et B.

  Pour obtenir des détails sur les comptes utilisateurs, voir *Administration basée sur les rôles à la page 12-2*.

Services

La conformité de la sécurité vérifie si les services clients OfficeScan suivants sont opérationnels :

- Antivirus
- Anti-spyware
- Pare-feu
- Réputation de sites Web
- Surveillance des comportements/Contrôle des dispositifs (également désignés par Service de prévention des modifications non autorisées Trend Micro)
- Protection des données

Un client non conforme est compté au minimum deux fois dans le rapport de conformité.

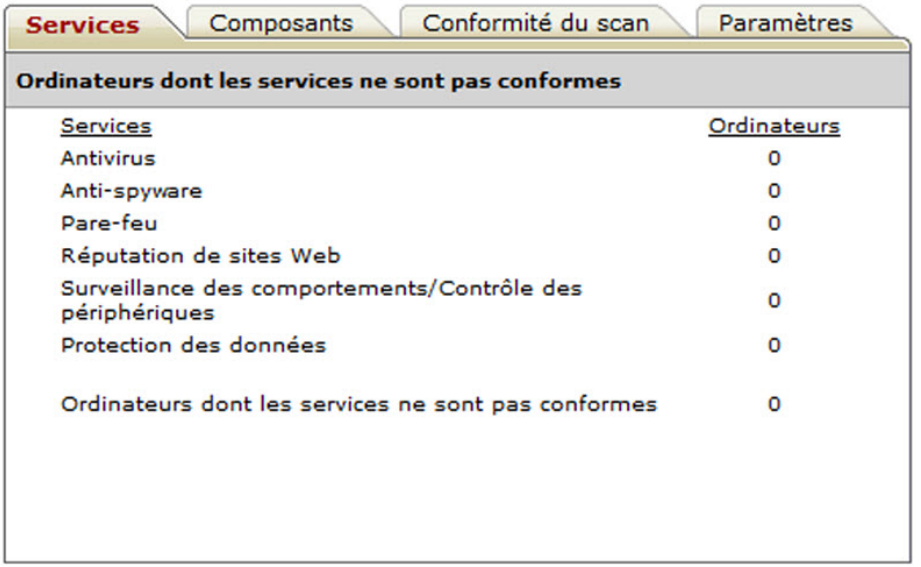


FIGURE 13-3. Rapport de conformité - onglet Services

- Dans la catégorie **Ordinateurs dont les services ne sont pas conformes**
- Dans la catégorie pour laquelle le client OfficeScan n'est pas conforme. Par exemple, si le service Antivirus du client OfficeScan n'est pas opérationnel, le client est compté dans la catégorie **Antivirus**. Si plusieurs services ne sont pas opérationnels, le client est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Redémarrez les services non opérationnels à partir de la console Web ou depuis l'ordinateur client OfficeScan. Si les services sont opérationnels après le redémarrage, le client n'apparaîtra plus comme non conforme lors de l'évaluation suivante.

Composants

La conformité de la sécurité détermine les incohérences de versions de composants entre le serveur OfficeScan et les clients OfficeScan. Ces incohérences se produisent généralement lorsque les clients ne peuvent pas se connecter au serveur pour mettre à jour les composants. Si le client obtient des mises à jour d'une autre source (telle que le serveur Trend Micro ActiveUpdate), il est possible que la version de composant d'un client soit plus récente que celle du serveur.

La conformité de la sécurité vérifie les composants suivants :

- Smart Scan Agent Pattern
- Fichier de signatures de virus
- Signatures IntelliTrap
- Signatures d'exceptions IntelliTrap
- Moteur de scan antivirus
- Signatures de spywares
- Signatures de surveillance active des spywares
- Moteur de scan anti-spyware
- Modèle de nettoyage de virus
- Moteur de nettoyage de virus
- Signatures du pare-feu commun
- Pilote du pare-feu commun
- Pilote de surveillance des comportements
- Service principal de surveillance des comportements
- Modèle de configuration de la surveillance des comportements
- Digital Signature Pattern
- Modèle de conformité aux stratégies
- Signatures de détection de l'analyse comportementale
- Version du programme

Un client non conforme est compté au minimum deux fois dans le rapport de conformité.

Rapport de conformité
Services
Composants
Conformité du scan
Paramètres
Ordinateurs disposant de versions des composants incohérentes
Composants
Ordinateurs
Smart Scan Agent Pattern 0
Fichier de signatures de virus 0
Signatures IntelliTrap 0
Signatures d'exceptions IntelliTrap 0
Moteur de scan antivirus 0
Signatures de spywares 0
Signatures de surveillance active des spywares 0
Moteur de scan anti-spyware 0
Modèle de nettoyage de virus 0
Moteur de nettoyage de virus 0
Signatures du pare-feu commun 0
Pilote du pare-feu commun 0
Pilote de surveillance des comportements 0

FIGURE 13-4. Rapport de conformité - onglet Composants

- Dans la catégorie **Ordinateurs disposant de versions des composants incohérentes**
- Dans la catégorie pour laquelle le client n'est pas conforme. Par exemple, si la version de Smart Scan Agent Pattern du client n'est pas cohérente avec le version du serveur, le client est compté dans la catégorie **Smart Scan Agent Pattern**. Si plusieurs versions de composants sont incohérentes, le client est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Pour résoudre les incohérences des versions des composants, mettez à jour les composants obsolètes sur les clients ou sur le serveur.

Conformité du scan

La conformité de la sécurité vérifie si le scan immédiat ou le scan programmé sont exécutés régulièrement et s'ils sont effectués dans un délai raisonnable.

Remarque

La conformité de la sécurité ne peut rapporter l'état du scan programmé que si le scan programmé est activé sur les clients.

La conformité de la sécurité utilise les critères de conformité du scan suivants :

- **Aucun scan immédiat ou programmé n'a été effectué dans les (x) derniers jours** : Un client OfficeScan n'est pas conforme s'il n'a pas exécuté de scan immédiat ou programmé dans le nombre de jours spécifié.
- **Le scan immédiat ou programmé a dépassé (x) heures** : Un client OfficeScan n'est pas conforme si la durée du dernier scan immédiat ou programmé a dépassé le nombre d'heures spécifié.

Un client non conforme est compté au minimum deux fois dans le rapport de conformité.

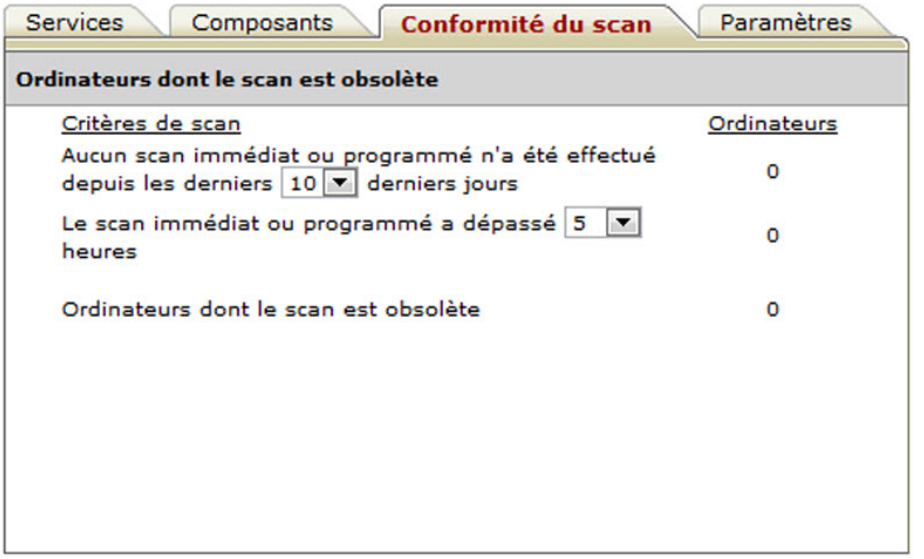


FIGURE 13-5. Rapport de conformité - onglet Conformité du scan

- Dans la catégorie **Ordinateurs dont le scan est obsolète**
- Dans la catégorie pour laquelle le client n'est pas conforme. Par exemple, si la durée du dernier scan programmé a dépassé le nombre d'heures spécifié, le client est compté dans la catégorie **Le scan immédiat ou programmé a dépassé <x> heures**. Si le client remplit plusieurs critères de conformité de scan, il est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Exécutez le scan immédiat ou le scan programmé sur les clients qui n'ont pas effectué de tâches de scan ou n'ont pas pu terminer le scan.

Paramètres

La conformité de la sécurité détermine si les clients ont les mêmes paramètres que leurs domaines parents dans l'arborescence client. Les paramètres peuvent être incohérents si

vous déplacez un client vers un autre domaine qui applique un ensemble de paramètres différent ou si un utilisateur client possédant certains privilèges a configuré manuellement des paramètres sur la console client OfficeScan.

OfficeScan vérifie les paramètres suivants :

- Méthode de scan
- Paramètres de scan manuel
- Paramètres de scan en temps réel
- Paramètres de scan programmé
- Paramètres de scan immédiat
- Privilèges et autres paramètres
- Paramètres des services complémentaires
- Réputation de sites Web
- Surveillance des comportements
- Contrôle des dispositifs
- Liste des spywares/graywares approuvés
- Paramètres de prévention contre la perte de données

Un client non conforme est compté au minimum deux fois dans le rapport de conformité.

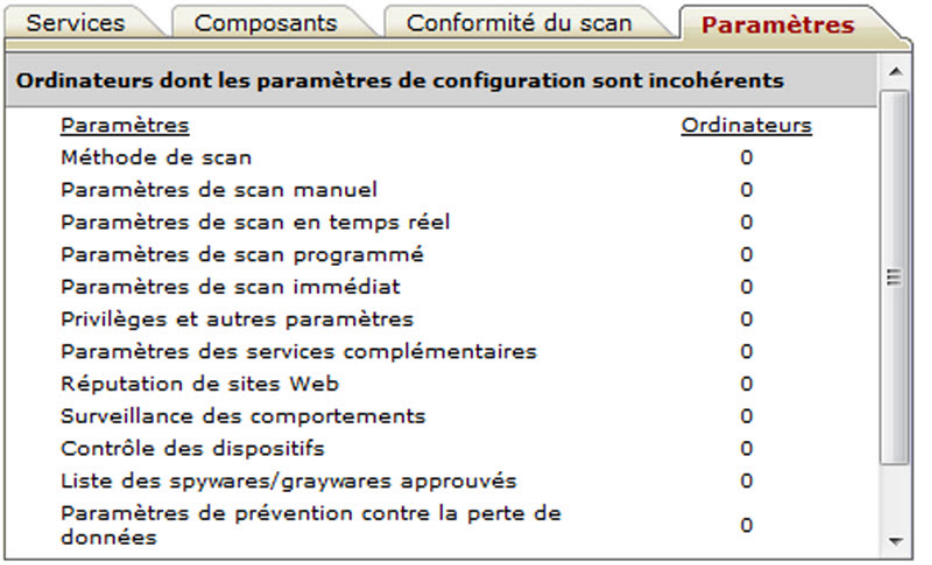


FIGURE 13-6. Rapport de conformité - onglet Paramètres

- Dans la catégorie **Ordinateurs dont les paramètres de configuration sont incohérents**
- Dans la catégorie pour laquelle le client n'est pas conforme. Par exemple, si les paramètres de méthode de scan d'un client et de son domaine parent ne sont pas cohérents, le client est compté dans la catégorie **Méthode de scan**. Si plusieurs ensembles de paramètres sont incohérents, le client est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Pour résoudre les incohérences de paramètres, appliquez au client les paramètres du domaine.

Rapports de conformité à la demande

La conformité de la sécurité peut générer des rapports de conformité à la demande. Les rapports vous permettent d'évaluer l'état de sécurité des clients OfficeScan gérés par le serveur OfficeScan.

Pour plus d'informations sur les rapports de conformité, consultez la rubrique *Conformité de la sécurité pour les clients gérés à la page 13-58*.

Génération d'un rapport de conformité à la demande

Tâche

1. Accédez à **Conformité de la sécurité** > **Évaluation de conformité** > **Rapport de conformité**.
2. Accédez à la section **Étendue de l'arborescence des clients**.
3. Sélectionnez un domaine ou le domaine racine et cliquez sur **Évaluer**.
4. Affichez le rapport de conformité pour les services du client.

   Pour plus d'informations concernant les services du client, voir *Services à la page 13-59*.

   a. Cliquez sur l'onglet **Services**.

   b. Sous **Ordinateurs dont les services ne sont pas conformes**, vérifiez le nombre de clients avec des services non conformes.

   c. Cliquez sur le lien d'un nombre pour afficher tous les clients concernés dans l'arborescence client.

   d. Sélectionnez les clients à partir des résultats de la requête.

   e. Cliquez sur **Redémarrer le client OfficeScan** pour redémarrer le service.

Remarque

Si, après avoir effectué une autre évaluation, le client apparaît encore comme non conforme, redémarrez manuellement le service sur l'ordinateur client.

f. Pour enregistrer la liste des clients dans un fichier, cliquez sur **Exporter**.

5. Affichez le rapport de conformité pour les composants du client.

   Pour plus d'informations sur les composants du client, voir *Composants à la page 13-61*.

   a. Cliquez sur l'onglet **Composants**.

   b. Sous **Ordinateurs disposant de versions des composants incohérentes**, vérifiez le nombre de clients avec des versions de composants incohérentes avec les versions du serveur.

   c. Cliquez sur le lien d'un nombre pour afficher tous les clients concernés dans l'arborescence client.

   Remarque

   Si l'un des clients possède un composant plus récent que le serveur OfficeScan, mettez le serveur à jour manuellement.

   d. Sélectionnez les clients à partir des résultats de la requête.

   e. Cliquez sur **Mettre à jour** pour forcer les clients à télécharger des composants.

   Remarque

   - Pour vous assurer que les clients peuvent mettre à niveau le programme client, désactivez l'option **Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client, ni déployer des correctifs de type hotfix** dans l'**Ordinateurs en réseau** > **Gestion des clients** > **Paramètres** > **Privilèges et autres paramètres**.
   - Redémarrez l'ordinateur au lieu de cliquer sur **Mettre à jour** pour mettre à jour le pilote du pare-feu commun.

   f. Pour enregistrer la liste des clients dans un fichier, cliquez sur **Exporter**.

6. Affichez le rapport de conformité pour les scans.

   Pour plus de détails sur les scans, voir *Conformité du scan à la page 13-63*.

a. Cliquez sur l'onglet **Conformité du scan**.

b. Sous **Ordinateurs dont le scan est obsolète**, configurez les paramètres suivants :

- Nombre de jours pendant lesquels un client n'a pas exécuté un scan immédiat ou un scan programmé
- Nombre d'heures depuis le début de l'exécution du scan immédiat ou programmé

Remarque

Si le nombre de jours ou d'heures est dépassé, le client est considéré comme non conforme.

c. Cliquez sur **Évaluer** à côté de la section **Étendue de l'arborescence des clients**.

d. Sous **Ordinateurs dont le scan est obsolète**, vérifiez le nombre de clients répondant aux critères de scan.

e. Cliquez sur le lien d'un nombre pour afficher tous les clients concernés dans l'arborescence client.

f. Sélectionnez les clients à partir des résultats de la requête.

g. Cliquez sur **Scan immédiat** pour lancer un scan immédiat chez le client.

Remarque

Pour éviter de recommencer le scan, l'option **Scan immédiat** sera désactivée si le scan immédiat a duré plus longtemps que le nombre d'heures spécifié.

h. Pour enregistrer la liste des clients dans un fichier, cliquez sur **Exporter**.

7. Affichez le rapport de conformité pour les paramètres.

Pour plus de détails sur les paramètres, voir *Paramètres à la page 13-64*.

a. Cliquez sur l'onglet **Paramètres**.

b. Sous **Ordinateurs dont les paramètres de configuration sont incohérents**, vérifiez le nombre de clients dont les paramètres sont incohérents avec les paramètres de domaine de l'arborescence client.

c. Cliquez sur le lien d'un nombre pour afficher tous les clients concernés dans l'arborescence client.

d. Sélectionnez les clients à partir des résultats de la requête.

e. Cliquez sur **Appliquer les paramètres de domaine**.

f. Pour enregistrer la liste des clients dans un fichier, cliquez sur **Exporter**.

Rapports de conformité planifiés

La conformité de la sécurité peut générer des rapports de conformité en fonction d'un calendrier. Les rapports vous permettent d'évaluer l'état de sécurité des clients OfficeScan gérés par le serveur OfficeScan.

Pour plus d'informations sur les rapports de conformité, consultez la rubrique *Conformité de la sécurité pour les clients gérés à la page 13-58*.

Configuration des paramètres pour les rapports de conformité programmés

Tâche

1. Accédez à **Conformité de la sécurité** > **Évaluation de conformité** > **Rapport de conformité planifié**.
2. Sélectionnez **Activer la génération de rapports programmés**.
3. Spécifiez le titre du rapport.
4. Sélectionnez tout ou partie des options suivantes :
   - *Services à la page 13-59*
   - *Composants à la page 13-61*
   - *Conformité du scan à la page 13-63*

- *Paramètres à la page 13-64*

5. Spécifiez les adresses e-mail auxquelles seront envoyées les notifications concernant les rapports de conformité programmés.

Remarque

Configurez les paramètres de notification par courrier électronique pour vous assurer que les notifications par courrier électronique seront envoyées correctement. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 12-32*.

6. Indiquez la programmation.

7. Cliquez sur **Enregistrer**.

Conformité de la sécurité pour les points finaux non gérés

La conformité de la sécurité peut interroger des points finaux non gérés dans le réseau auquel le serveur OfficeScan appartient. Utilisez Active Directory et les adresses IP pour interroger des points finaux.

L'état de sécurité des points finaux non gérés peut être l'un des suivants :

TABLEAU 13-8. État de sécurité des points finaux non gérés

ÉTAT	DESCRIPTION
Géré par un autre serveur OfficeScan	Les clients OfficeScan installés sur les ordinateurs sont gérés par un autre serveur OfficeScan. Les clients OfficeScan sont en ligne et exécutent cette version d'OfficeScan ou une version antérieure.
Aucun client OfficeScan installé	Le client OfficeScan n'est pas installé sur l'ordinateur.
Non accessible	Le serveur OfficeScan ne parvient pas à se connecter à l'ordinateur, ni à déterminer son état de sécurité.

ÉTAT	DESCRIPTION
Évaluation d'Active Directory non résolue	L'ordinateur appartient à un domaine Active Directory, mais le serveur OfficeScan est incapable de déterminer son état de sécurité. **Remarque** La base de données du serveur OfficeScan contient une liste de clients gérés par le serveur. Le serveur interroge Active Directory pour obtenir les GUID des ordinateurs et les compare ensuite à ceux enregistrés dans la base de données. Si un GUID ne figure pas dans la base de données, l'ordinateur sera rangé dans la catégorie Évaluation d'Active Directory non résolue.

Pour lancer une évaluation de la sécurité, effectuez les tâches suivantes :

1. Définissez l'étendue de la requête. Pour obtenir des informations détaillées, voir *Définition de l'étendue d'Active Directory/ des adresses IP et de la requête. à la page 13-72*.
2. Vérifiez les ordinateurs non protégés à partir du résultat de la requête. Pour obtenir des informations détaillées, voir *Affichage des résultats de la requête à la page 13-75*.
3. Installez le logiciel client OfficeScan. Pour obtenir des informations détaillées, voir *Installation avec la conformité à la sécurité à la page 4-61*.
4. Configurez les requêtes programmées. Pour obtenir des informations détaillées, voir *Configuration l'évaluation de la requête programmée à la page 13-76*.

Définition de l'étendue d'Active Directory/des adresses IP et de la requête.

Lorsque vous effectuez une requête pour la première fois, définissez l'étendue d'Active Directory/des adresses IP, qui comprend les objets Active Directory et les adresses IP que le serveur OfficeScan interrogera à la demande ou périodiquement. Une fois l'étendue définie, lancez le processus d'interrogation.

Remarque

Pour définir une étendue Active Directory, Office Scan doit d'abord être intégré à Active Directory. Pour plus de détails sur l'intégration, voir *Intégration d'Active Directory à la page 2-27*.

Tâche

1. Accédez à **Conformité de la sécurité** > **Gestion des serveurs externes**.
2. Dans la section **Étendue Active Directory/adresse IP**, cliquez sur **Définir**. Un nouvel écran s'affiche.
3. Pour définir une étendue d'Active Directory :
   a. Accédez à la section **Étendue Active Directory**.
   b. Sélectionnez **Utiliser les évaluations à la demande** afin d'effectuer des requêtes en temps réel et de parvenir à des résultats plus précis. Lorsque cette option est désactivée, OfficeScan interroge la base de données, et non chaque client OfficeScan. Interroger uniquement la base de données s'avère plus rapide, mais également moins précis.
   c. Sélectionnez les objets à interroger. Si vous effectuez la requête pour la première fois, sélectionnez un objet comportant moins de 1,000 comptes et notez le temps nécessaire à l'exécution de la requête. Utilisez ces données comme point de référence pour les performances.
4. Pour définir une étendue des adresses IP :
   a. Accédez à la section **Étendue d'adresses IP**.
   b. Sélectionnez **Activer Étendue d'adresses IP**.
   c. Spécifiez une plage d'adresses IP. Cliquez sur le bouton plus ou moins pour ajouter ou supprimer des plages d'adresses IP.
   - Pour un serveur OfficeScan IPv4 pur, saisissez une plage d'adresses IPv4.
   - Pour un serveur OfficeScan IPv6 pur, saisissez un préfixe et une longueur IPv6.

- Pour un serveur OfficeScan double pile, saisissez une plage d'adresses IPv4 et/ou un préfixe et une longueur IPv6.

  La plage d'adresses IPv6 est limitée à 16 bits, ce qui est similaire aux plages d'adresses IPv4. La longueur du préfixe doit ainsi être comprise entre 112 et 128.

  TABLEAU 13-9. Longueurs de préfixe et nombre d'adresses IPv6

LONGUEUR	NOMBRE D'ADRESSES IPV6
128	2
124	16
120	256
116	4,096
112	65,536

5. Sous Paramètre avancés, spécifiez les ports utilisés par les serveurs OfficeScan pour communiquer avec les clients. Le programme d'installation génère de manière aléatoire le numéro de port pendant l'installation du serveur OfficeScan.

   Pour afficher le port de communication utilisé par le serveur OfficeScan, accédez à l'**Ordinateurs en réseau** > **Gestion des clients** et sélectionnez un domaine. Le port s'affiche en regard de la colonne d'adresse IP. Trend Micro vous recommande de noter les numéros de port à titre de référence.

   a. Cliquez sur **Spécifier les ports**.

   b. Saisissez le numéro de port et cliquez sur **Ajouter**. Reprenez cette opération jusqu'à ce que tous les numéros de port que vous souhaitez ajouter s'affichent.

   c. Cliquez sur **Enregistrer**.

6. Pour vérifier la connectivité d'un ordinateur en utilisant un numéro de port particulier, sélectionnez **Déclarer un ordinateur inaccessible en vérifiant le port <x>**. Si la connexion n'est pas établie, OfficeScan considère immédiatement que l'ordinateur est inaccessible. Le numéro de port par défaut est 135.

   L'activation de ce paramètre accélère la requête. Lorsqu'il ne parvient pas à établir la communication avec un ordinateur, le serveur OfficeScan n'a plus besoin

d'effectuer toutes les autres tâches de vérification de la connexion avant de considérer un ordinateur comme inaccessible.

7. Pour enregistrer l'étendue et lancer la requête, cliquez **Enregistrer et réévaluer**. Pour enregistrer uniquement les paramètres, cliquez sur **Enregistrer uniquement**. L'écran Gestion des serveurs externes affiche le résultat de la requête.

Remarque

La requête risque de prendre un certain temps, notamment si son étendue est importante. Ne lancez pas une autre requête tant que l'écran Gestion des serveurs externes n'affiche pas les résultats. Autrement, la session de requête actuelle prendra fin et le processus de requête redémarrera.

Affichage des résultats de la requête

Le résultat de la requête apparaît sous la section État de sécurité. Un point final non géré aura l'un des états suivants :

- Géré par un autre serveur OfficeScan
- Aucun client OfficeScan installé
- Non accessible
- Évaluation d'Active Directory non résolue

Tâches recommandées

1. Dans la section **État de sécurité**, cliquez sur un lien numérique pour afficher tous les ordinateurs affectés.
2. Utilisez les fonctions de recherche et de recherche avancée pour rechercher et afficher uniquement les ordinateurs qui répondent aux critères de recherche.

   Si vous utilisez la fonction de recherche avancée, spécifiez les éléments suivants :

   - Plage d'adresses IPv4
   - Préfixe et longueur IPv6 (le préfixe doit être compris entre 112 et 128)
   - Nom de l'ordinateur

- Nom du serveur OfficeScan
- Arborescence Active Directory
- État de sécurité

OfficeScan ne renvoie pas de résultat si le nom est incomplet. Vous pouvez utiliser un caractère générique (*) en cas de doute sur le nom complet.

3. Pour enregistrer la liste d'ordinateurs dans un fichier, cliquez sur **Exporter**.
4. Pour les clients OfficeScan gérés par un autre serveur OfficeScan, utilisez l'outil Client Mover pour que ces clients OfficeScan soient gérés par le serveur OfficeScan actuel. Voir *Client Mover à la page 13-23* pour obtenir des informations complémentaires sur cet outil.

Configuration l'évaluation de la requête programmée

Configurez le serveur OfficeScan pour interroger périodiquement Active Directory et les adresses IP afin de garantir que les stratégies de sécurité sont appliquées.

Tâche

1. Accédez à **Conformité de la sécurité** > **Gestion des serveurs externes**.
2. Cliquez sur **Paramètres** en haut de l'arborescence client.
3. Activez la fonction de requête programmée.
4. Indiquez la programmation.
5. Cliquez sur **Enregistrer**.

Trend Micro Virtual Desktop Support

Optimisez la protection des bureaux virtuels en utilisant Trend Micro Virtual Desktop Support. Cette fonctionnalité régule les tâches sur les clients OfficeScan qui résident sur un serveur virtuel unique.

L'exploitation de plusieurs bureaux sur un seul serveur et l'exécution de scans à la demande ou de mises à jour de composants consomment une quantité importante de

ressources système. Utilisez cette fonctionnalité pour empêcher les clients d'exécuter simultanément des scans ou des mises à jour de composants.

Par exemple, si un serveur VMware vCenter possède trois bureaux virtuels exécutant des clients OfficeScan, OfficeScan peut déclencher un scan immédiat et déployer simultanément des mises à jour sur les trois clients. Virtual Desktop Support détecte la présence des clients sur le même serveur physique. Virtual Desktop Support autorise le déroulement d'une tâche sur le premier client et en retarde l'exécution sur les deux autres tant que la tâche n'est pas terminée sur le premier client.

Virtual Desktop Support peut être utilisé sur les plates-formes suivantes :

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

Pour plus d'informations sur ces plates-formes, consultez les sites Web VMware View, Citrix XenDesktop ou Microsoft Hyper-V.

Utilisez l'outil OfficeScan de génération de modèle de pré-scan VDI pour optimiser les scans à la demande ou supprimer des GUID des images de base ou Golden.

Installation de Virtual Desktop Support

Virtual Desktop Support est une fonctionnalité native d'OfficeScan, mais nécessite une licence séparée. Après avoir installé le serveur OfficeScan, cette fonctionnalité est disponible, mais pas opérationnelle. L'installation de cette fonctionnalité implique le téléchargement d'un fichier depuis le serveur ActiveUpdate (ou depuis une source de mise à jour personnalisée, si définie). Une fois le fichier intégré au serveur OfficeScan, vous pouvez activer Virtual Desktop Support pour que cette fonctionnalité soit totalement opérationnelle. L'installation et l'activation sont exécutées à partir de Plug-In Manager.

Remarque

Virtual Desktop Support n'est pas complètement pris en charge dans les environnements en IPv6 pur. Pour obtenir des informations détaillées, voir *Limitations des serveurs IPv6 purs à la page A-3*.

Installation de Virtual Desktop Support

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Dans l'écran **Plug-in Manager**, accédez à la section **Trend Micro Virtual Desktop Support** et cliquez sur **Télécharger**.

   La taille du pack s'affiche en regard du bouton **Télécharger**.

   Plug-In Manager stocke le pack téléchargé dans <*le dossier d'installation du serveur*>`\PCCSRV\Télécharger\Produit`.

   Remarque

   Si Plug-In Manager le téléchargement du fichier n'est pas possible, il est relancé automatiquement après 24 heures. Pour déclencher manuellement Plug-In Manager pour télécharger le pack, redémarrez le service OfficeScanPlug-In Manager à partir de la console d'administration Microsoft Management Console.

3. Surveillez la progression du téléchargement. Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

   Si vous rencontrez des problèmes lors du téléchargement du pack, consultez les journaux de mise à jour du serveur sur la console du produit OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Journaux de mise à jour du serveur**.

   Une fois que Plug-In Manager télécharge le fichier, Virtual Desktop Support s'affiche dans une nouvelle fenêtre.

   Remarque

   Si Virtual Desktop Support ne s'affiche pas, consultez les causes et les solutions dans *Dépannage de Plug-In Manager à la page 14-10*.

4. Pour installer Virtual Desktop Support immédiatement, cliquez sur **Installer**. Pour installer ultérieurement :

   a. Cliquez sur **Installer ultérieurement**.

   b. Ouvrez la fenêtre **Plug-in Manager**.

   c. Accédez à la section **Trend Micro Virtual Desktop Support**, puis cliquez sur **Installer**.

5. Lisez attentivement le contrat de licence, puis acceptez ses termes en cliquant sur **Accepter**.

   L'installation démarre.

6. Surveillez la progression de l'installation. Après l'installation, la version de Virtual Desktop Support s'affiche.

Licence de Virtual Desktop Support

Affichez, activez et renouvelez la licence de Virtual Desktop Support à partir du Plug-In Manager.

Obtenez le code d'activation auprès de Trend Micro, puis utilisez-le pour activer les fonctionnalités complètes de Virtual Desktop Support.

Activation ou renouvellement de Virtual Desktop Support

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Sur l'écran **Plug-in Manager**, accédez à la section **Trend Micro Virtual Desktop Support** et cliquez sur **Manage Program**.
3. Cliquez sur **Afficher les informations de licence**.
4. Sur l'écran qui s'affiche, **Détails sur la licence du produit** cliquez sur **Nouveau code d'activation**.

5. Sur l'écran qui s'affiche, saisissez le code d'activation puis cliquez sur **Enregistrer**.

6. Lorsque vous revenez à l'écran Détails sur la licence du produit, cliquez sur **Informations sur la mise à jour** pour actualiser l'écran avec les nouvelles informations sur la licence et l'état de la fonction. Cet écran fournit également un lien vers le site Web de Trend Micro sur lequel vous trouverez des informations détaillées relatives à votre licence.

Affichage des informations relatives à la licence de Virtual Desktop Support

Tâche

1. Ouvrez la console Web OfficeScan et cliquez sur **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.

2. Cliquez sur **Afficher les informations de licence**.

3. Consultez les informations relatives à la licence dans l'écran qui s'ouvre.

   La section Détails de la licence de Virtual Desktop Support fournit les informations suivantes :

   - **État** : affiche « Activé », « Non activé » ou « Expiré ».
   - **Version** : affiche la version « complète » ou la version d'« évaluation ». Si vous disposez à la fois de la version complète et de la version d'évaluation, la version qui s'affiche alors est la version « complète ».
   - **Date d'expiration** : Si Virtual Desktop Support dispose de plusieurs licences, la dernière date d'expiration s'affiche. Par exemple, si les dates d'expiration de la licence sont le 31/12/2010 et le 30/06/2010, la date qui s'affiche est le 31/12/2010.
   - **Postes** : Affiche le nombre de clients OfficeScan pouvant utiliser Virtual Desktop Support
   - **Code d'activation** : affiche le code d'activation

   Des messages de rappel concernant les licences s'affichent dans les cas suivants:

Si vous possédez une licence de version complète :

- Pendant la période de grâce de la fonction. La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro.
- Une fois la licence expirée et la période de grâce écoulée: pendant cette période, vous ne pourrez pas obtenir d'assistance technique.

Si vous disposez de la licence de la version d'évaluation

- Une fois la licence expirée: pendant cette période, vous ne pourrez pas obtenir d'assistance technique.

4. Cliquez sur **Afficher le détail de la licence en ligne** pour afficher les informations relatives à votre licence sur le site Web de Trend Micro.
5. Pour rafraîchir l'écran avec les dernières informations de licence, cliquez sur **Informations sur la mise à jour**.

Connexions Virtual Server

Optimisez les scans à la demande ou les mises à jour de composants en ajoutant VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4) ou Microsoft Hyper-V Server. Les serveurs OfficeScan communiquent avec les serveurs virtuels indiqués pour identifier les clients OfficeScan qui résident sur le même serveur physique.

Ajout de connexions serveur

Tâche

1. Ouvrez la console Web OfficeScan et cliquez sur **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.
2. Sélectionnez **Serveur VMware vCenter**, **Citrix XenServer** ou**Microsoft Hyper-V**.
3. Activez la connexion au serveur.

4. Indiquez les informations suivantes :

   - Pour les serveurs VMware vCenter et Citrix XenServer :
     - adresse IP
     - Port
     - Protocole de connexion (HTTP ou HTTPS)
     - Nom d'utilisateur
     - Mot de passe
   - Pour les serveurs Microsoft Hyper-V :
     - Nom ou adresse IP de l'hôte
     - Domaine\Nom d'utilisateur

     Remarque

     Le compte de connexion doit être un compte de domaine dans le groupe Administrateurs

     - Mot de passe

5. Activez éventuellement la connexion proxy pour VMware vCenter ou Citrix XenServer.

   a. Indiquez le nom ou l'adresse IP et le numéro de port du serveur proxy.

   b. Si le serveur proxy nécessite une authentification, indiquez le nom d'utilisateur et le mot de passe appropriés.

6. Cliquez sur **Tester la connexion** pour vérifier que le serveur OfficeScan se connecte correctement au serveur.

Remarque

Pour plus d'informations sur les connexions Microsoft Hyper-V, consultez *Dépannage des connexions Microsoft Hyper-V à la page 13-83*.

7. Cliquez sur **Enregistrer**.

Ajout de plusieurs connexions serveur

Tâche

1. Ouvrez la console Web OfficeScan et cliquez sur **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.
2. Cliquez sur **Ajouter une connexion vCenter**, **Ajouter une connexion XenServer** ou sur **Ajouter une connexion Hyper-V**.
3. Reprenez la procédure permettant de fournir les informations de serveur appropriées.
4. Cliquez sur **Enregistrer**.

Suppression d'un paramètre de connexion

Tâche

1. Ouvrez OfficeScan Web Console, puis accédez à **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.
2. Cliquez sur **Supprimer cette connexion**.
3. Cliquez sur **Ok** pour confirmer la suppression de ce paramètre.
4. Cliquez sur **Enregistrer**.

Dépannage des connexions Microsoft Hyper-V

La connexion Microsoft Hyper-V utilise WMI (Windows Management Instrumentation) et DCOM pour la communication client-serveur. Les stratégies de pare-feu peuvent bloquer cette communication, entraînant ainsi l'échec de la connexion au serveur Hyper-V.

Le port d'écoute du serveur Hyper-V est, par défaut, défini sur le port 135 et sélectionne de façon aléatoire un port configuré pour une communication ultérieure. Si le pare-feu bloque le trafic WMI ou l'un de ces deux ports, la communication avec le serveur échoue. Les administrateurs peuvent modifier la stratégie du pare-feu pour permettre une bonne communication avec le serveur Hyper-V.

Vérifiez que tous les paramètres de connexion, notamment l'adresse IP, le domaine, le nom d'utilisateur et le mot de passe sont corrects avant d'effectuer les modifications du pare-feu suivantes.

Permettre la communication WMI via le pare-feu Windows

Tâche

1. Sur le serveur Hyper-V, ouvrez la fenêtre **Programmes autorisés du pare-feu Windows**.

   Sur les systèmes Windows 2008 R2, accédez à **panneau de configuration** > **système et sécurité** > **pare-feu Windows** > **autorise un programme ou une fonction via le pare-feu Windows**.

2. Sélectionnez **Windows Management Instrumentation (WMI)**.

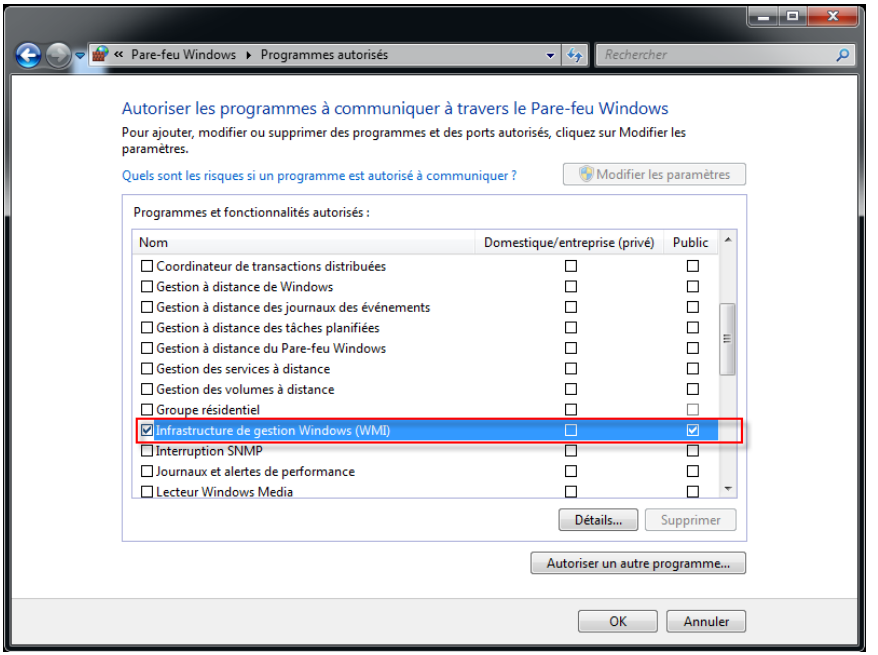

« Pare-feu Windows ▸ Programmes autorisés
Rechercher
Autoriser les programmes à communiquer à travers le Pare-feu Windows
Pour ajouter, modifier ou supprimer des programmes et des ports autorisés, cliquez sur Modifier les paramètres.
Quels sont les risques si un programme est autorisé à communiquer ?
Modifier les paramètres
Programmes et fonctionnalités autorisés :
Nom
Domestique/entreprise (privé)
Public
Coordinateur de transactions distribuées
Gestion à distance de Windows
Gestion à distance des journaux des événements
Gestion à distance des tâches planifiées
Gestion à distance du Pare-feu Windows
Gestion des services à distance
Gestion des volumes à distance
Groupe résidentiel
Infrastructure de gestion Windows (WMI)
Interruption SNMP
Journaux et alertes de performance
Lecteur Windows Media
Détails...
Supprimer
Autoriser un autre programme...
OK
Annuler

FIGURE 13-7. Programme d'écran autorisé du pare-feu Windows

3. Cliquez sur **Enregistrer**.

4. Testez à nouveau la connexion Hyper-V.

Ouverture du port de communication via le pare-feu Windows ou un pare-feu tiers

Tâche

1. Sur le serveur Hyper-V, assurez-vous que le pare-feu permet la communication via le port 135 puis testez la connexion Hyper-V à nouveau.

   Pour des informations supplémentaires concernant l'ouverture des ports, reportez-vous à votre documentation de pare-feu.

2. Si la connexion au serveur Hyper-V échoue, configurez WMI pour utiliser un port fixe.

Pour plus d'informations concernant *configuration d'un port fixe pour WMI*, reportez-vous à :

http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. Ouvrez les ports 135 et le port fixe nouvellement créé (24158) pour une communication via le pare-feu.

4. Testez à nouveau la connexion Hyper-V.

Outil de génération de modèle de pré-scan VDI

Utilisez l'outil OfficeScan de génération de modèle de pré-scan VDI pour optimiser les scans à la demande ou supprimer des GUID des images de base ou Golden. Cet outil scanne l'image de base ou Golden et la certifie. Lorsque le scan duplique l'image, OfficeScan vérifie uniquement les parties qui ont été modifiées. Le délai de scan est ainsi réduit.

Conseil

Trend Micro recommande de générer le modèle de pré-scan après une mise à jour Windows ou après l'installation d'une nouvelle application.

Création d'un modèle de pré-scan

Tâche

1. Sur l'ordinateur du serveur OfficeScan, accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Choisissez une version de l'outil de génération de modèle de pré-scan VDI. Les versions suivantes sont à votre disposition :

TABLEAU 13-10. Versions de l'outil de génération de modèle de pré-scan VDI

NOM DU FICHIER	INSTRUCTION
TCacheGen.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 32 bits.
TCacheGen_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 64 bits.
TCacheGenCli.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 32 bits.
TCacheGenCli_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 64 bits.

3. Copiez la version de l'outil que vous avez choisi à l'étape précédente dans le <*dossier d'installation du client*> de l'image de base.

4. Exécutez l'outil.

   - Pour exécuter l'outil directement :

     a. Double-cliquez sur `TCacheGen.exe` ou `TCacheGen_x64.exe`.

     b. Cliquez sur **Générer un modèle de pré-scan**.

   - Pour exécuter l'outil depuis l'interface de ligne de commande :

     a. Ouvrez une invite de commande et modifiez le répertoire en `<dossier d'installation du client>`.

     b. Saisissez la commande suivante :

     ```
     TCacheGenCli Generate_Template
     ```

     Ou

     ```
     TcacheGenCli_x64 Generate_Template
     ```

Remarque

Avant de générer le modèle de pré-scan et de supprimer le GUID, l'outil scanne l'image pour détecter d'éventuelles menaces de sécurité.

Une fois le modèle de pré-scan généré, l'outil décharge le client OfficeScan. Ne rechargez pas le client OfficeScan. Si celui-ci se recharge, vous devrez recréer le modèle de pré-scan.

Suppression de GUID des modèles

Tâche

1. Sur l'ordinateur du serveur OfficeScan, accédez au <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Choisissez une version de l'outil de génération de modèle de pré-scan VDI. Les versions suivantes sont à votre disposition :

TABLEAU 13-11. Versions de l'outil de génération de modèle de pré-scan VDI

NOM DU FICHIER	INSTRUCTION
TCacheGen.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 32 bits.
TCacheGen_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 64 bits.
TCacheGenCli.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 32 bits.
TCacheGenCli_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 64 bits.

3. Copiez la version de l'outil que vous avez choisi à l'étape précédente dans le <*dossier d'installation du client*> de l'image de base.

4. Exécutez l'outil.

   - Pour exécuter l'outil directement :

a. Double-cliquez sur `TCacheGen.exe` ou `TCacheGen_x64.exe`.

b. Cliquez sur **Supprimer le GUID du modèle**.

- Pour exécuter l'outil depuis l'interface de ligne de commande :

a. Ouvrez une invite de commande et modifiez le répertoire en `<dossier d'installation du client>`.

b. Saisissez la commande suivante :

```
TCacheGenCli Remove GUID
```

Ou

```
TcacheGenCli_x64 Remove GUID
```

Paramètres clients généraux

OfficeScan applique les paramètres clients généraux à tous les clients ou seulement aux clients disposant de certains privilèges.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Configurez les paramètres suivants :

TABLEAU 13-12. Paramètres clients généraux

PARAMÈTRE	RÉFÉRENCE
Paramètres de scan	*Paramètres de scan généraux à la page 6-69*
Paramètres de scan programmé	*Paramètres de scan généraux à la page 6-69*
Paramètres de bande passante des journaux de virus/programmes malveillants	*Paramètres de scan généraux à la page 6-69*

PARAMÈTRE	RÉFÉRENCE
Paramètres du pare-feu	*Paramètres généraux du pare-feu à la page 11-27*
Nombre d'entrées du journal du pare-feu	*Paramètres généraux du pare-feu à la page 11-27*
Paramètres de surveillance des comportements	*Surveillance des comportements à la page 7-2*
Mises à jour	*Serveur ActiveUpdate comme source de mise à jour du client OfficeScan à la page 5-36*
Espace disque réservé	*Configuration de l'espace disque réservé pour les mises à jour clients OfficeScan à la page 5-49*
Réseau inaccessible	*Clients inaccessibles à la page 13-45*
Paramètres d'alerte	*Configuration des notifications de mise à jour du client OfficeScan à la page 5-51*
Redémarrage d'OfficeScan Service	*Redémarrage des services du client OfficeScan à la page 13-12*
Configuration proxy	*Paramètres proxy automatique pour le client OfficeScan à la page 13-53*
Adresse IP de votre choix	*Adresses IP du client à la page 4-8*

3. Cliquez sur **Enregistrer**.

Configuration des privilèges clients et autres paramètres

Accordez aux utilisateurs les privilèges de modification de certains paramètres et de réalisation des tâches de haut niveau sur le client OfficeScan.

Remarque

Les paramètres antivirus n'apparaissent uniquement qu'après activation de la fonctionnalité antivirus OfficeScan.

Conseil

Pour garantir l'uniformité des paramètres et des stratégies dans l'ensemble de l'entreprise, accordez aux utilisateurs des privilèges limités.

Tâche

1. Accédez à **Ordinateurs en réseau** > **Paramètres clients généraux** ou **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, configurez les privilèges utilisateur suivants :

TABLEAU 13-13. Privilèges client

PRIVILÈGES CLIENT	RÉFÉRENCE
Privilège de mode itinérance	*Privilège des clients OfficeScan itinérants à la page 13-20*
Privilèges de scan	*Privilèges de type de scan à la page 6-53*
Privilèges de scan programmé	*Privilèges et autres paramètres de scan programmé à la page 6-56*
Privilèges du pare-feu	*Privilèges du pare-feu à la page 11-24*
Privilèges de surveillance des comportements	*Privilèges de surveillance des comportements à la page 7-10*
Privilèges du scan de courrier	*Privilèges et autres paramètres du scan de courrier à la page 6-62*
Privilèges de la boîte à outils	*Accord de privilège d'affichage de l'onglet Boîte à outils pour les utilisateurs à la page 16-7*
Privilèges de paramètres proxy	*Privilèges de configuration proxy pour les clients à la page 13-52*

Privilèges client	Référence
Privilèges de mise à jour des composants	*Mettre à jour les privilèges et autres paramètres pour les clients OfficeScan à la page 5-46*
Désinstallation	*Autorisation du privilège de désinstallation du client OfficeScan à la page 4-72*
Déchargement	*Accord de privilège de déchargement du client à la page 13-19*

5. Cliquez sur l'onglet **Autres paramètres**, puis configurez les paramètres suivants :

Tableau 13-14. Autres paramètres clients

Paramètre	Référence
Paramètres de mise à jour	*Mettre à jour les privilèges et autres paramètres pour les clients OfficeScan à la page 5-46*
Paramètres de réputation de sites Web	*Notifications sur les menaces Internet pour les utilisateurs clients à la page 10-10*
Paramètres de surveillance des comportements	*Privilèges de surveillance des comportements à la page 7-10*
Autoprotection client	*Autoprotection client à la page 13-13*
Paramètres du cache pour les scans	*Paramètres du cache pour les scans à la page 6-65*
Paramètres de scan programmé	*Attribution de privilèges de scan programmé et affichage de la notification de privilège à la page 6-57*
Paramètres de sécurité du client	*Sécurité du client OfficeScan à la page 13-17*
Paramètres de scan de la messagerie POP3	*Attribution des privilèges du scan de courrier et activation du scan de la messagerie POP3 à la page 6-64*
Accès restreint à la console client	*Restriction de l'accès à la console client OfficeScan à la page 13-18*

PARAMÈTRE	RÉFÉRENCE
Notification de redémarrage	*Notifications sur les risques liés à la sécurité pour les utilisateurs du client OfficeScan à la page 6-83*

6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Chapitre 14

Utilisation de Plug-In Manager

Ce chapitre explique comment configurer Plug-In Manager et présente les solutions de plugiciel fournies via Plug-In Manager.

Sujets abordés dans ce chapitre :

- *À propos de Plug-In Manager à la page 14-2*
- *Installation de Plug-In Manager à la page 14-3*
- *Gestion des fonctionnalités natives d'OfficeScan à la page 14-4*
- *Gestion des plugiciels à la page 14-4*
- *Désinstallation de Plug-In Manager à la page 14-9*
- *Dépannage de Plug-In Manager à la page 14-10*

À propos de Plug-In Manager

OfficeScan inclut une structure appelée Plug-In Manager qui intègre les nouvelles solutions dans l'environnement OfficeScan existant. Pour faciliter la gestion de ces solutions, Plug-In Manager permet de voir en un coup d'œil les données correspondant aux solutions, sous forme de widgets.

Remarque

Actuellement, aucune des solutions de plug-in ne prend en charge IPv6. Le serveur peut télécharger ces solutions mais ne peut pas les déployer sur des clients OfficeScan IPv6 purs ou des hôtes IPv6 purs.

Plug-In Manager fournit deux types de solutions :

- **Fonctions natives d'OfficeScan**

  Certaines fonctions natives d'OfficeScan possèdent une licence séparée et sont activées via Plug-In Manager. Dans cette version, deux fonctions entrent dans cette catégorie, respectivement **Trend Micro Virtual Desktop Support** et **Protection des données OfficeScan**.

- **Programmes plug-in**

  Les programmes de plug-in ne font pas partie du programme OfficeScan. Ces programmes possèdent leurs propres licences et sont gérés principalement depuis leurs propres consoles de gestion, accessibles depuis la console Web OfficeScan. **Intrusion Defense Firewall**, **Sécurité Trend Micro (pour Mac)**, et **Trend Micro Mobile Security** sont des exemples de plugiciels.

Ce document fournit une présentation générale de l'installation et de la gestion des plug-ins et aborde les données relatives aux plug-ins disponibles dans les widgets. Reportez-vous à la documentation du programme de plug-in spécifique pour plus d'informations sur la configuration et la gestion du programme.

Agents côté client et Plug-in Manager client

Certains plugiciels (comme Intrusion Defense Firewall) possèdent un agent côté client qui s'installe sur les systèmes d'exploitation Windows. Les agents côté clients peuvent être gérés via un client Plug-in Manager exécutant le processus `CNTAoSMgr.exe`.

`CNTAoSMgr.exe` est installé avec le client OfficeScan et possède les mêmes exigences système. Seul un programme supplémentaire est requis pour `CNTAoSMgr.exe` : Microsoft XML Parser (MSXML) version 3.0 ou ultérieure.

Remarque

Les autres agents côté client ne sont pas installés sous des systèmes d'exploitation Windows et ils ne sont dès lors pas gérés par le client Plug-in Manager. Le client Trend Micro Security (pour Mac) et l'agent dispositif Mobile pour Trend Micro Mobile Security font partie de ces agents.

Widgets

Utilisez les widgets pour voir d'un coup d'oeil les données pour les solutions de plug-in individuelles que vous avez déployées. Les widgets sont disponibles sur le tableau de bord récapitulatif du serveur OfficeScan. Un widget spécial, appelé **Mashup d'OfficeScan et des plug-ins**, combine les données des clients OfficeScan et les solutions de plug-in, puis présente les données dans l'arborescence des clients.

Le Manuel de l'administrateur fournit une présentation générale des widgets et des solutions qui prennent les widgets en charge.

Installation de Plug-In Manager

Dans les versions précédentes de Plug-In Manager, le pack d'installation de Plug-In Manager est téléchargé à partir de Trend Micro ActiveUpdate server, puis installé sur l'ordinateur qui héberge le serveur OfficeScan. Dans cette version, le pack d'installation de Plug-in Manager est compris dans le pack d'installation du serveur OfficeScan.

Après avoir exécuté le pack et effectué l'installation, les utilisateurs débutant avec OfficeScan auront installé à la fois le serveur OfficeScan et Plug-In Manager. Les

utilisateurs qui mettent à niveau leur version d'OfficeScan et ont déjà utilisé Plug-In Manager devront arrêter le service Plug-In Manager avant d'exécuter le pack d'installation.

Exécution de tâches après l'installation

Après avoir installé Plug-In Manager, procédez de la manière suivante :

Tâche

1. Accédez à la console Web Plug-In Manager en cliquant sur **Plug-in Manager** dans le menu principal d'OfficeScan Web Console.
2. Gérez les solutions de plug-in.
3. Accédez au tableau de bord récapitulatif de la console Web OfficeScan pour gérer les widgets pour les solutions de plug-in.

Gestion des fonctionnalités natives d'OfficeScan

Les fonctionnalités natives d'OfficeScan sont installées avec OfficeScan et activées depuis Plug-In Manager. Certaines fonctionnalités, telles que Trend Micro Virtual Desktop Support, sont gérées depuis Plug-In Manager alors que d'autres, telles qu'Protection des données OfficeScan, sont gérées depuis OfficeScan Web Console.

Gestion des plugiciels

Installez et activez les plugiciels indépendamment d'OfficeScan. Chaque plugiciel fournit sa propre console pour la gestion du produit. Les consoles d'administration sont accessibles depuis OfficeScan Web Console.

Installation de plug-ins

Un plugiciel apparaît sur la console Plug-In Manager. À partir de la console, vous pouvez télécharger, installer et gérer le programme. Plug-In Manager télécharge le pack d'installation d'un plugiciel à partir de Trend Micro ActiveUpdate Server ou d'une source de mise à jour personnalisée, si une source a été correctement configurée. Une connexion Internet est nécessaire pour télécharger le pack depuis le serveur ActiveUpdate.

Lorsque Plug-In Manager télécharge un pack d'installation ou lance une installation, les fonctions des autres plugiciels (téléchargements, installations et mises à niveau) sont temporairement désactivées par Plug-In Manager.

Plug-In Manager ne prend pas en charge l'installation et la gestion d'un plugiciel via la fonction d'authentification unique de Trend Micro Control Manager.

Installation d'un plugiciel

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Sur l'écran Plug-in Manager, accédez à la section des plugiciels et cliquez sur **Télécharger**. La taille du pack du plugiciel s'affiche en regard du bouton **Télécharger**. Plug-in Manager stocke le pack téléchargé dans `<Dossier d'installation du serveur>\PCCSRV\Download\Product`.
3. Surveillez la progression du téléchargement. Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

Téléchargement de Trend Micro Mobile Security
Veuillez patienter pendant le téléchargement de Trend Micro Mobile Security version 5.5.1122. Vous pouvez accéder à d'autres pages d'OfficeScan pendant le téléchargement.
Progression : 11%
< Retour

FIGURE 14-1. Progression du téléchargement d'un plugiciel

Une fois le fichier téléchargé par Plug-in Manager, le plugiciel s'affiche dans une nouvelle fenêtre.

Remarque

Si vous rencontrez des problèmes lors du téléchargement du pack, consultez les journaux de mise à jour du serveur sur la console du produit OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Journaux de mise à jour du serveur**.

4. Cliquez sur **Installer maintenant** ou **Installer plus tard**.

   - Si vous avez cliqué sur **Installer maintenant**, vérifiez la progression de l'installation.
   - Si vous avez cliqué sur **Installer plus tard**, rendez-vous dans la fenêtre Plug-in Manager, puis dans la section du plugiciel et cliquez sur **Installer**. Vérifiez ensuite la progression de l'installation.

Une fois l'installation terminée, la version du plugiciel s'affiche. Vous pouvez ensuite commencer à gérer le plugiciel.

Gestion des plug-ins

Configurez les paramètres et réalisez des tâches relatives à la console de gestion des plug-ins, accessible depuis la console Web OfficeScan. Ces tâches comprennent notamment l'activation du programme et le déploiement de son agent côté client sur les points finaux. Consultez la documentation spécifique du plug-in pour plus d'informations sur la configuration et la gestion du programme.

Gestion d'un plugiciel

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager**.
2. Sur l'écran **Plug-in Manager**, accédez à la section des plugiciels et cliquez sur **Gestion de programme**.

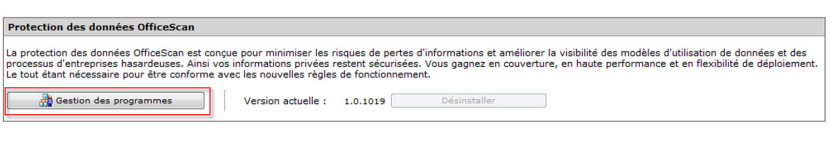

Protection des données OfficeScan
La protection des données OfficeScan est conçue pour minimiser les risques de pertes d'informations et améliorer la visibilité des modèles d'utilisation de données et des processus d'entreprises hasardeuses. Ainsi vos informations privées restent sécurisées. Vous gagnez en couverture, en haute performance et en flexibilité de déploiement. Le tout étant nécessaire pour être conforme avec les nouvelles règles de fonctionnement.
Gestion des programmes
Version actuelle : 1.0.1019
Désinstaller

FIGURE 14-2. Bouton de gestion de plug-in

Mises à niveau de plug-ins

La nouvelle version d'un plugiciel installé s'affiche dans la console de Plug-In Manager. Dans la console, vous pouvez télécharger le pack de mise à niveau, puis mettre à niveau le programme. Plug-In Manager télécharge les packs des plugiciels à partir de Trend Micro ActiveUpdate Server ou d'une source de mise à jour personnalisée, si une source a été correctement configurée. Une connexion Internet est nécessaire pour télécharger le pack depuis le serveur ActiveUpdate.

Lorsque Plug-In Manager télécharge un pack d'installation ou lance une mise à niveau, les fonctions des autres plugiciels (téléchargements, installations et mises à niveau) sont temporairement désactivées par Plug-In Manager.

Plug-In Manager ne prend pas en charge la mise à niveau d'un plugiciel via la fonction d'authentification unique de Trend Micro Control Manager.

Mise à niveau d'un plugiciel

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Sur l'écran **Plug-in Manager**, accédez à la section des plugiciels et cliquez sur **Télécharger**. La taille du pack de mise à niveau s'affiche en regard du bouton **Télécharger**.
3. Surveillez la progression du téléchargement. Il est possible de naviguer vers un autre écran pendant le téléchargement, sans incidence sur la mise à niveau.

Remarque

Si vous rencontrez des problèmes lors du téléchargement du pack, consultez les journaux de mise à jour du serveur sur OfficeScan Web Console. Dans le menu principal, cliquez sur **Journaux** > **Journaux de mise à jour du serveur**.

4. Une fois que Plug-In Manager a terminé le téléchargement du pack, un nouvelle fenêtre s'affiche.

5. Cliquez sur **Mettre à niveau maintenant** ou **Mettre à niveau plus tard**.

   - Si vous avez cliqué sur **Mettre à niveau maintenant**, vérifiez la progression de la mise à niveau.

   - Si vous avez cliqué sur **Mettre à niveau plus tard**, accédez à la fenêtre **Plug-in Manager**, puis cliquez sur **Mettre à niveau** dans la section des plugiciels. Vérifiez ensuite la progression de la mise à niveau.

Une fois la mise à niveau terminée, un redémarrage du service Plug-In Manager sera peut-être nécessaire. La fenêtre Plug-in Manager sera alors momentanément indisponible. Lorsque l'écran redevient disponible, la version actuelle du plugiciel s'affiche.

Désinstallation de plug-ins

Il existe plusieurs façons de désinstaller un plug-in.

- Désinstallation du plugiciel à partir de la console Plug-In Manager.

- Désinstallation du serveur OfficeScan, qui génère la désinstallation de Plug-In Manager et de tous les plugiciels installés. Pour obtenir des instructions sur la désinstallation du serveur OfficeScan, consultez le *Guide d'installation et de mise à niveau OfficeScan*.

Concernant les plug-ins qui ont des agents côté client :

- Consultez la documentation relative au plug-in pour savoir si la désinstallation du plug-in entraîne également la désinstallation de l'agent côté client.

- Quant aux agents côté client installés sur le même ordinateur que le client OfficeScan, la désinstallation du client OfficeScan entraîne la désinstallation des agents côté client et du client Plug-in Manager (`CNTAoSMgr.exe`).

Désinstallation d'un plugiciel à partir de la console Plug-In Manager.

Tâche

1. Ouvrez OfficeScan Web Console, puis cliquez sur **Plug-in Manager** dans le menu principal.
2. Sur l'écran **Plug-in Manager**, accédez à la section des plugiciels, puis cliquez sur **Désinstaller**.

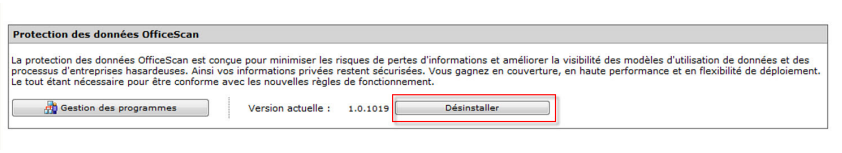

Protection des données OfficeScan
La protection des données OfficeScan est conçue pour minimiser les risques de pertes d'informations et améliorer la visibilité des modèles d'utilisation de données et des processus d'entreprises hasardeuses. Ainsi vos informations privées restent sécurisées. Vous gagnez en couverture, en haute performance et en flexibilité de déploiement. Le tout étant nécessaire pour être conforme avec les nouvelles règles de fonctionnement.
Gestion des programmes
Version actuelle : 1.0.1019
Désinstaller

FIGURE 14-3. Bouton Désinstaller d'un plugiciel

3. Surveillez la progression de la désinstallation. Vous pouvez naviguer dans une autre fenêtre pendant l'opération.
4. Actualisez l'écran **Plug-in Manager** après la désinstallation. Le plug-in est à nouveau prêt à être installé.

Désinstallation de Plug-In Manager

Désinstallez le serveur OfficeScan afin de désinstaller Plug-In Manager et tous les plugiciels installés. Pour obtenir des instructions sur la désinstallation du serveur OfficeScan, consultez le *Guide d'installation et de mise à niveau OfficeScan*.

Dépannage de Plug-In Manager

Consultez les journaux de débogage du client OfficeScan et du serveur OfficeScan pour obtenir des informations sur le débogage de Plug-In Manager et des plugiciels.

Un plugiciel ne s'affiche pas dans la console de Plug-in Manager

Un plugiciel téléchargeable et installable peut ne pas s'afficher dans la console de Plug-In Manager pour les raisons suivantes :

Tâche

1. Plug-In Manager est toujours en train de télécharger le plugiciel. Le téléchargement peut prendre du temps selon la taille du pack du programme. Vérifiez l'écran de temps à autre pour voir si le plugiciel apparaît.

   Remarque

   Si Plug-In Manager n'est pas en mesure de télécharger un plugiciel, il procède à une nouvelle tentative au bout de 24 heures. Pour déclencher le téléchargement manuel du plugiciel par Plug-In Manager, redémarrez le service OfficeScanPlug-In Manager.

2. Le serveur ne peut pas se connecter à Internet. Si l'ordinateur serveur se connecte à Internet par le biais d'un serveur proxy, assurez-vous que la connexion Internet peut être établie avec les paramètres du proxy.

3. La source de mise à jour OfficeScan n'est pas le serveur ActiveUpdate. Dans la console Web OfficeScan, accédez à **Mises à jour** > **Serveur** > **Source de mise à jour** et vérifiez la source de mise à jour. Si la source de mise à jour ne correspond pas au serveur ActiveUpdate, plusieurs possibilités vous sont offertes :

   - Sélectionnez le serveur ActiveUpdate comme source de mise à jour.
   - Si vous sélectionnez **Autre source de mise à jour**, sélectionnez la première entrée comme source de mise à jour dans la liste **Autres sources de mise à jour**, puis vérifiez que la source peut correctement se connecter au serveur ActiveUpdate. Plug-In Manager ne prend en charge que la première entrée de la liste.

- Si vous sélectionnez **Emplacement Intranet contenant une copie du fichier actuel**, assurez-vous que l'ordinateur sur l'Intranet peut également se connecter au serveur ActiveUpdate.

Problèmes d'installation et d'affichage côté client de l'agent

L'installation d'un plug-in côté client de l'agent peut échouer ou l'agent peut ne pas s'afficher dans la console du client OfficeScan pour les raisons suivantes :

Tâche

1. Plug-in Manager côté client (`CNTAosMgr.exe`) ne fonctionne pas. Dans l'ordinateur client OfficeScan, ouvrez le Gestionnaire de tâches et exécutez le processus `CNTAosMgr.exe`.
2. Le pack d'installation pour l'agent côté client n'a pas été téléchargé dans le dossier de l'ordinateur client OfficeScan situé dans `<Dossier d'installation du client >\AU_Data\AU_Temp\{xxx}AU_Down\Product`. Consultez `Tmudump.txt` situé dans `\AU_Data\AU_Log\` pour connaître les raisons de l'échec du téléchargement.

   Remarque

   Si un agent est installé avec succès, des informations sur cet agent sont disponibles dans `<Dossier d'installation du client>\AOSSvcInfo.xml`.

3. L'installation de l'agent a échoué ou nécessite d'autres actions. Vous pouvez vérifier l'état de l'installation à partir de la console d'administration des plugiciels et procéder à un redémarrage de l'ordinateur client OfficeScan à la fin de l'installation, ou encore installer les mises à jour système avant de procéder à l'installation.

Cette version du serveur Web Apache n'est pas prise en charge

Plug-In Manager traite certaines requêtes Internet à l'aide de l'interface ISAPI (Internet Server Application Programming Interface). L'interface ISAPI n'est pas compatible avec le serveur Web Apache versions 2.0.56 à 2.0.59 et versions 2.2.3 à 2.2.4.

Si vous avez une version incompatible du serveur Web Apache, vous pouvez le remplacer par la version 2.0.63, qui est utilisée par OfficeScan et Plug-In Manager. Cette version est également compatible avec l'interface ISAPI.

Tâche

1. Mettez à niveau le serveur OfficeScan vers la version actuelle.
2. Sauvegardez les fichiers suivants dans le dossier Apache2 du `<Dossier d'installation du serveur>`:
   - `httpd.conf`
   - `httpd.conf.tmbackup`
   - `httpd.default.conf`
3. Désinstallez la version incompatible du serveur Web Apache depuis l'écran **Ajout/Suppression de programmes**.
4. Installez le serveur Web Apache 2.0.63
   a. Lancez `apache.msi` à partir de `<Dossier d'installation du serveur>\Admin\Utility\Apache`.
   b. Dans l'écran relatif aux informations du serveur, entrez les informations demandées.
   c. Dans l'écran Dossier de destination, modifiez le dossier de destination en cliquant sur **Modifier** et en accédant à `<Dossier d'installation du serveur>`.
   d. Terminez l'installation.
5. Copiez les fichiers de sauvegarde dans le dossier Apache2.

6. Redémarrez le service serveur Web Apache.

Un agent côté client ne peut pas être lancé si la configuration du script de configuration automatique dans Internet Explorer redirige vers un serveur proxy

Le client Plug-in Manager (`CNTAosMgr.exe`) ne peut pas lancer un agent côté client parce que la commande de lancement de l'agent entraîne une redirection vers un serveur proxy. Le problème ne survient que si les paramètres proxy redirigent le trafic HTTP de l'utilisateur vers le port 127.0.0.1.

Pour résoudre ce problème, utilisez une stratégie de serveur proxy bien définie. Par exemple, ne redirigez pas le trafic HTTP vers le port 127.0.0.1.

Si vous devez utiliser la configuration proxy contrôlant les requêtes HTTP 127.0.0.1, effectuez les tâches suivantes :

Tâche

1. Configurez les paramètres du pare-feu OfficeScan dans la console Web OfficeScan.

   Remarque

   Réalisez cette opération si vous activez le pare-feu OfficeScan sur les clients OfficeScan.

   a. Dans la console Web, accédez à **Ordinateurs en réseau** > **Pare-feu** > **Stratégies** et cliquez sur **Modifier le modèle d'exception**.

   b. Dans l'écran Modifier le modèle d'exception, cliquez sur **Ajouter**.

   c. Utilisez les informations suivantes :

      - **Nom**: le nom de votre choix
      - **Action** : Autoriser le trafic réseau
      - **Direction** : Entrant
      - **Protocole**: TCP

- **Port(s)** : tout numéro de port compris entre 5000 et 49151

d. **Adresse(s) IP** : sélectionnez **Adresse IP unique** et spécifiez l'adresse IP de votre serveur proxy (recommandé) ou sélectionnez **Toutes les adresses IP**.

e. Cliquez sur **Enregistrer**.

f. De retour dans l'écran Modifier le modèle d'exception, cliquez sur **Enregistrer et appliquer aux stratégies existantes**.

g. Accédez à **Ordinateurs en réseau** > **Pare-feu** > **Profils** et cliquez sur **Affecter un profil aux clients**.

S'il n'existe pas de profil de pare-feu, créez-en un en cliquant sur Ajouter. Utilisez les paramètres suivants :

- **Nom**: le nom de votre choix
- **Description** : la description de votre choix
- **Stratégie** : toutes les stratégies d'accès

Une fois le nouveau profil enregistré, cliquez sur **Affecter un profil aux clients**.

2. Modifiez le fichier `ofcscan.ini`.

a. Ouvrez le fichier `ofcscan.ini` situé dans le `<dossier d'installation du serveur>` via un éditeur de texte.

b. Recherchez **`[Global Setting]`** et ajoutez `FWPortNum=21212` à la ligne suivante. Remplacez la valeur « 21212 » par le numéro de port précédemment spécifié à l'étape c.

Par exemple :

```
[Global Setting]

FWPortNum=5000
```

c. Enregistrez le fichier.

3. Dans la console Web, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux** et cliquez sur **Enregistrer**.

Une erreur s'est produite dans le système, le module de mise à jour ou le programme Plug-in Manager et le message d'erreur fournit un certain code d'erreur

Plug-In Manager affiche l'un des codes d'erreur suivants dans un message d'erreur. Si vous ne parvenez pas à résoudre un problème après avoir consulté les solutions proposées dans le tableau ci-dessous, adressez-vous à votre service d'assistance.

TABLEAU 14-1. Codes d'erreur Plug-In Manager

CODE D'ERREUR	MESSAGE, CAUSE ET SOLUTION
001	Une erreur est survenue dans le programme Plug-In Manager. Le module de mise à jour de Plug-In Manager ne répond pas lors de l'interrogation de la progression d'une tâche de mise à jour. Le gestionnaire de commande ou de module n'a peut-être pas été initialisé. Redémarrez le service OfficeScanPlug-In Manager et effectuez cette tâche à nouveau.
002	Une erreur système est survenue. Le module de mise à jour Plug-In Manager ne parvient pas à ouvrir la clé de registre `SOFTWARE\TrendMicro\OfficeScan\service\AoS` parce qu'elle a été supprimée. Effectuez les actions suivantes : 1. Ouvrez l'Éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Redéfinissez la valeur sur 1.0.1000. 2. Redémarrez le service OfficeScanPlug-In Manager. 3. Téléchargez/désinstallez le plug-in.

CODE D'ERREUR	MESSAGE, CAUSE ET SOLUTION
028	Une erreur de mise à jour est survenue. Causes possibles : • Le module de mise à jour de Plug-In Manager n'a pas pu télécharger un plugiciel. Vérifiez que la connexion réseau fonctionne correctement, puis réessayez. • Le module de mise à jour de Plug-In Manager ne peut pas installer le plugiciel car l'agent du patch AU a renvoyé une erreur. L'agent du patch AU est le programme qui lance l'installation des nouveaux plugiciels. Pour connaître la cause exacte de l'erreur, consultez le journal de débogage du module « `TmuDump.txt` » dans `\PCCSRV\Web\Service\AU_Data\AU_Log`. Effectuez les actions suivantes : 1. Ouvrez l'Éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Redéfinissez la valeur sur 1.0.1000. 2. Supprimez la clé de registre du plugiciel `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`. 3. Redémarrez le service OfficeScanPlug-In Manager. 4. Téléchargez et installez le plugiciel.
170	Une erreur système est survenue. Le module de mise à jour de Plug-In Manager ne peut pas traiter d'opération entrante car il est actuellement en train de traiter une autre opération. Veuillez effectuer cette tâche ultérieurement.
202	Une erreur est survenue dans le programme Plug-In Manager. Plug-In Manager ne peut pas traiter une tâche en cours d'exécution sur la console Web. Actualisez la console Web ou mettez à niveau Plug-In Manager si une mise à niveau est disponible.

CODE D'ERREUR	MESSAGE, CAUSE ET SOLUTION
203	Une erreur est survenue dans le programme Plug-In Manager. Le programme Plug-In Manager a rencontré une erreur de communication inter-processus (IPC) lors d'une tentative de communication avec les services back-end de Plug-In Manager. Redémarrez le service OfficeScanPlug-In Manager et effectuez cette tâche à nouveau.
Autres codes d'erreur	Une erreur système est survenue. En téléchargeant un nouveau plugiciel, Plug-In Manager vérifie la liste des plugiciels à partir du serveur ActiveUpdate. Plug-In Manager n'a pas pu obtenir la liste. Effectuez les actions suivantes : 1. Ouvrez l'Éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Redéfinissez la valeur sur `1.0.1000`. 2. Redémarrez le service OfficeScanPlug-In Manager. 3. Téléchargez et installez le plugiciel.

Chapitre 15

Utilisation de Policy Server pour Cisco NAC

ce chapitre comprend des instructions de base destinées à installer et à configurer le serveur Policy Server for Cisco NAC. Pour obtenir de plus amples informations relatives à la configuration et à l'administration des serveurs Cisco Secure ACS et autres produits Cisco, veuillez consulter la documentation Cisco la plus récente disponible sur le site Web suivant:

http://www.cisco.com/univercd/home/home.htm

Sujets abordés dans ce chapitre :

- *À propos de Policy Server pour Cisco NAC à la page 15-3*
- *Composants et terminologie à la page 15-3*
- *Architecture Cisco NAC à la page 15-7*
- *Séquence de validation du client à la page 15-8*
- *Serveur Policy Server à la page 15-10*
- *Configuration minimale requise pour le serveur Policy Server à la page 15-22*
- *Configuration requise pour Cisco Trust Agent (CTA) à la page 15-23*
- *Plates-formes prises en charge et configuration requise à la page 15-24*

- *Déploiement de Policy Server for NAC à la page 15-25*

À propos de Policy Server pour Cisco NAC

Le serveur Trend Micro Policy Server for Cisco Network Admission Control (NAC) permet d'évaluer l'état des composants antivirus des clients OfficeScan. Les options de configuration du serveur Policy Server vous permettent de configurer les paramètres afin d'effectuer des actions sur des clients à risque, de manière à les rendre conformes aux stratégies de sécurité de la société.

Ces actions sont :

- Demande de mise à jour des composants client OfficeScan aux clients OfficeScan
- Activation du scan en temps réel
- Exécuter l'option Scan immédiat
- Afficher un message de notification sur les ordinateurs clients OfficeScan informant les utilisateurs en cas de violation de la stratégie antivirus

Pour plus d'informations sur la technologie Cisco NAC, consultez le site Web Cisco à l'adresse suivante :

http://www.cisco.com/go/nac

Composants et terminologie

Vous trouverez ci-dessous la liste des divers composants et des termes importants avec lesquels vous devez vous familiariser afin de comprendre et d'utiliser le serveur Policy Server for Cisco NAC.

Composants

Les composants suivants sont nécessaires pour la mise en œuvre Trend Micro du serveur Policy Server for Cisco NAC°:

TABLEAU 15-1. Composants du serveur Policy Server for Cisco NAC

COMPOSANT	DESCRIPTION
Cisco Trust Agent (CTA)	Programme installé sur un ordinateur client pour lui permettre de communiquer avec d'autres composants Cisco NAC.
Ordinateur client OfficeScan	Ordinateur sur lequel est installé le programme client OfficeScan. Pour utiliser Cisco NAC, l'ordinateur client OfficeScan nécessite également l'installation de Cisco Trust Agent.
Périphérique d'accès au réseau	Périphérique réseau qui prend en charge la fonctionnalité Cisco NAC. Les périphériques d'accès au réseau pris en charge comprennent des routeurs Cisco, des pare-feux, des points d'accès, ainsi que des dispositifs tiers configurés avec le protocole TACACS+ (Terminal Access Controller Access Control System) ou le protocole RADIUS (Remote Dial-In User Service). Voir *Plates-formes prises en charge et configuration requise à la page 15-24* pour obtenir la liste des dispositifs pris en charge.
Cisco Secure Access Control Server (ACS)	Serveur qui reçoit les données antivirus du client OfficeScan par l'intermédiaire du périphérique d'accès au réseau et les transmet à une base de données externe d'utilisateurs pour évaluation. A un stade ultérieur du processus, le serveur ACS transmet également au périphérique d'accès au réseau le résultat de l'évaluation, qui peut comprendre des instructions à l'intention du client OfficeScan.
Policy Server	Programme qui reçoit et évalue les données antivirus du client OfficeScan. Une fois l'évaluation effectuée, le serveur Policy Server détermine les actions que le client OfficeScan doit exécuter puis envoie une notification au client OfficeScan lui demandant d'exécuter les actions.
Serveur OfficeScan	Indique au serveur Policy Server les versions actuelles des fichiers de signatures de virus et de moteur de scan antivirus. Ces informations sont utilisées par le serveur Policy Server pour évaluer l'état de l'antivirus du client OfficeScan.

Terminologie

Familiarisez-vous avec la terminologie suivante liée au serveur Policy Server for Cisco NAC°:

TABLEAU 15-2. Conditions du serveur Policy Server for Cisco NAC

TERME	DÉFINITION
État de sécurité	Présence et actualité du logiciel antivirus sur un client OfficeScan. Dans cet emploi, l'état de sécurité consiste à vérifier la présence du programme client OfficeScan sur les ordinateurs clients, l'état de certains paramètres du client OfficeScan et l'état de mise à jour du moteur de scan antivirus et des fichiers de signatures de virus.
Jeton d'état	Créé par le serveur Policy Server après la validation du client OfficeScan. Il comprend des informations indiquant que le client OfficeScan peut exécuter des actions spécifiées telles que l'activation du scan en temps réel ou la mise à jour des composants antivirus.
Validation du client	Processus qui consiste à évaluer l'état de sécurité du client et à renvoyer le jeton d'état au client OfficeScan.
Règle de serveur Policy Server	Directives contenant les critères de configuration utilisés par le serveur Policy Server, afin de mesurer l'état de sécurité d'un client OfficeScan. Une règle contient également des actions que le client OfficeScan et le serveur Policy Server doivent exécuter si les informations sur l'état de sécurité correspondent aux critères (pour plus d'informations, consultez *Stratégies et règles du serveur Policy Server à la page 15-11*).
Stratégie de serveur Policy Server	Ensemble de règles du serveur Policy Server avec lesquelles il mesure l'état de sécurité des clients OfficeScan. Les stratégies contiennent également des actions que les clients OfficeScan et le serveur Policy Server exécutent si les critères des règles associées à la stratégie ne correspondent pas à l'état de sécurité (pour plus d'informations, consultez *Stratégies et règles du serveur Policy Server à la page 15-11*).

TERME	DÉFINITION
authentification, autorisation et mesure (AAA)	Les trois principaux services utilisés pour contrôler l'accès du client de l'utilisateur final OfficeScan aux ressources informatiques. Authentification : identification d'un client, en général par saisie d'un nom d'utilisateur et d'un mot de passe. Autorisation : privilèges d'exécution de certaines commandes accordés à l'utilisateur. Mesure : mesure des ressources utilisées pendant une session, en général consignée dans des journaux. Cisco Secure Access Control Server (ACS) est l'application par Cisco d'un serveur AAA.
autorité de certification (CA)	Autorité du réseau qui distribue les certificats numériques dans le but d'authentifier et de sécuriser les connexions entre ordinateurs et/ou serveurs.
Certificats numériques	Pièce jointe servant à la sécurité. Le plus souvent, les certificats authentifient les clients auprès des serveurs tels que des serveurs Web. Ils contiennent les éléments suivants : informations sur l'identité de l'utilisateur, un code public (pour le codage) et la signature numérique d'une autorité de certification (CA) pour vérifier la validité du certificat.
Remote Authentication Dial-In User Service (RADIUS)	Système d'authentification demandant aux clients de saisir un nom d'utilisateur et un mot de passe. Les serveurs Cisco Secure ACS prennent en charge RADIUS.
Terminal Access Controller Access Control System (TACACS+)	Protocole de sécurité activé par l'intermédiaire des commandes AAA utilisées pour l'authentification des clients des utilisateurs finaux. Les serveurs Cisco ACS prennent en charge TACACS+.

Architecture Cisco NAC

Le diagramme suivant montre une architecture Cisco NAC de base.

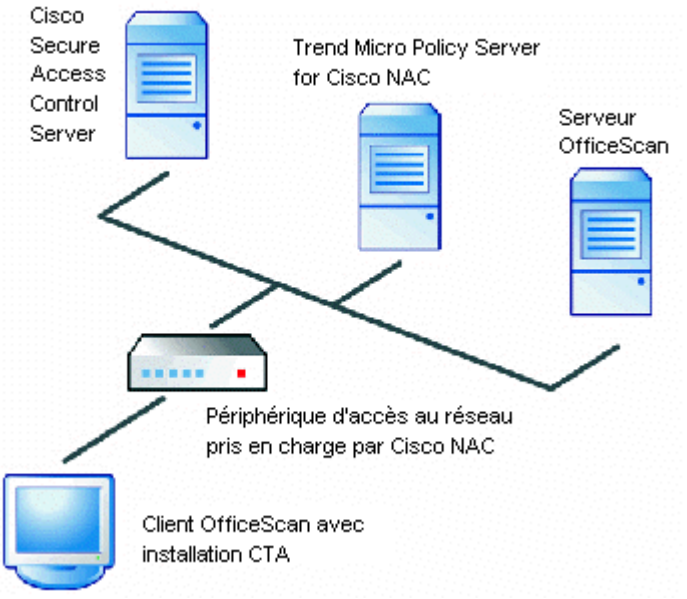


FIGURE 15-1. Architecture Cisco NAC de base

Dans cette illustration, le client OfficeScan présente une installation CTA et peut uniquement accéder au réseau par le biais d'un périphérique d'accès au réseau prenant en charge Cisco NAC. Le périphérique d'accès au réseau se trouve entre le client et les autres composants Cisco NAC.

Remarque

l'architecture de votre réseau peut être différente, en fonction de la présence ou pas de serveurs proxy, de routeurs ou de pare-feu.

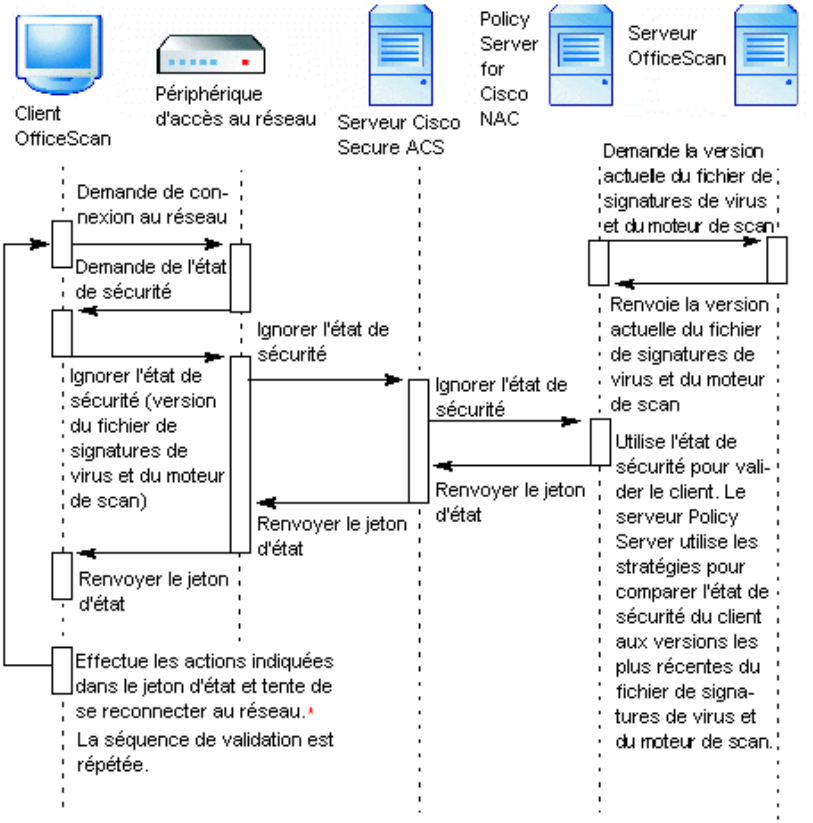
Séquence de validation du client

La validation du client OfficeScan désigne le processus consistant à évaluer l'état de sécurité d'un client OfficeScan et à renvoyer des instructions à exécuter par le client OfficeScan si le serveur Policy Server considère qu'il est exposé à un risque. Le serveur Policy Server valide un client OfficeScan à l'aide de règles et de stratégies configurables.

La séquence des événements qui se produisent lorsqu'un client OfficeScan tente d'accéder au réseau est indiquée ci-dessous°:

1. Le périphérique d'accès au réseau Cisco lance la séquence de validation en se renseignant sur l'état de sécurité du client lorsqu'il tente d'accéder au réseau.
2. Le périphérique d'accès au réseau transmet alors l'état de sécurité au serveur ACS.
3. Le serveur ACS transmet également l'état de sécurité au serveur Policy Server qui procède à une évaluation.
4. Dans un processus distinct, le serveur Policy Server interroge périodiquement le serveur OfficeScan pour obtenir des informations relatives à la version du fichier de signatures de virus et du moteur de scan antivirus afin de maintenir ses données à jour. Il utilise alors une stratégie que vous configurez afin de comparer ces informations avec les données de l'état de sécurité du client OfficeScan.
5. Ensuite, le serveur Policy Server créé un jeton d'état et le renvoie au client OfficeScan.

6. Le client OfficeScan exécute sur lui-même les actions configurées dans le jeton d'état.


Client OfficeScan
Périphérique d'accès au réseau
Serveur Cisco Secure ACS
Policy Server for Cisco NAC
Serveur OfficeScan
Demande de connexion au réseau
Demande de l'état de sécurité
Ignorer l'état de sécurité
Ignorer l'état de sécurité (version du fichier de signatures de virus et du moteur de scan)
Ignorer l'état de sécurité
Renvoyer le jeton d'état
Renvoyer le jeton d'état
Demande la version actuelle du fichier de signatures de virus et du moteur de scan
Renvoie la version actuelle du fichier de signatures de virus et du moteur de scan
Utilise l'état de sécurité pour valider le client. Le serveur Policy Server utilise les stratégies pour comparer l'état de sécurité du client aux versions les plus récentes du fichier de signatures de virus et du moteur de scan.
Renvoyer le jeton d'état
Effectue les actions indiquées dans le jeton d'état et tente de se reconnecter au réseau.*
La séquence de validation est répétée.

* Le client essaie d'accéder de nouveau au réseau lorsque le temporisateur du périphérique d'accès au réseau arrive à expiration. Reportez-vous à la documentation relative au routeur Cisco pour obtenir de plus amples informations sur la configuration du temporisateur.

FIGURE 15-2. Séquence de validation d'accès au réseau

Serveur Policy Server

Le serveur Policy Server évalue l'état de sécurité du client OfficeScan et crée le jeton d'état. Il compare l'état de sécurité aux dernières versions du fichier de signatures de virus et du moteur de scan antivirus envoyées par le serveur OfficeScan dont le client OfficeScan est membre. Il renvoie le jeton d'état au serveur Cisco Secure ACS, qui le transmet lui-même au client OfficeScan par l'intermédiaire du périphérique d'accès au réseau Cisco.

L'installation de serveurs Policy Server supplémentaires sur un réseau unique peut améliorer les performances lorsqu'un grand nombre de clients tentent d'accéder simultanément au réseau. Ces serveurs Policy Server peuvent également servir de sauvegarde lorsqu'un serveur Policy Server devient inutilisable. Si plusieurs serveurs OfficeScan sont installés sur un réseau, le serveur Policy Server traite les demandes de tous les serveurs OfficeScan enregistrés sur ce réseau. De même, plusieurs serveurs Policy Server peuvent traiter des demandes d'un serveur OfficeScan unique enregistré

sur tous les serveurs Policy Server. La figure ci-dessous illustre la relation entre plusieurs serveurs OfficeScan et serveurs Policy Server.

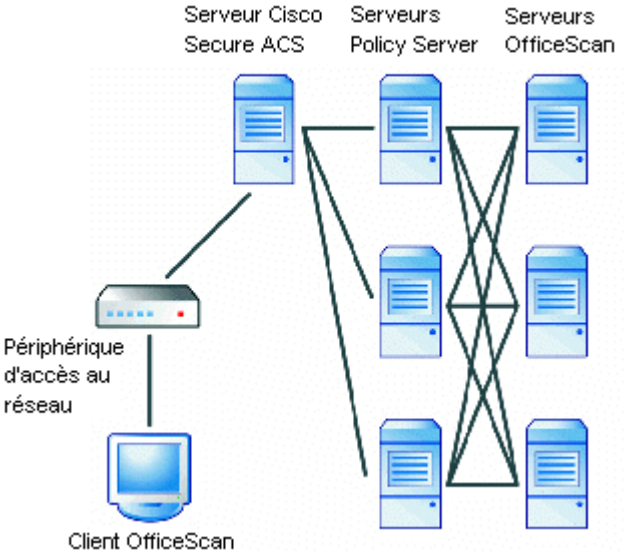


FIGURE 15-3. Relation entre plusieurs serveurs OfficeScan et serveurs Policy Server

Vous pouvez aussi installer le serveur Policy Server sur le même ordinateur que le serveur OfficeScan.

Stratégies et règles du serveur Policy Server

Les serveurs Policy Server utilisent des stratégies et des règles configurables pour favoriser l'application des stratégies et des consignes de sécurité de votre entreprise.

Les règles comprennent des critères spécifiques que les serveurs Policy Server comparent à l'état de sécurité des clients OfficeScan. Si l'état de sécurité du client correspond aux critères configurés dans une règle, le client et le serveur exécutent les actions spécifiées dans la règle (voir *Actions du client OfficeScan et du serveur Policy Server à la page 15-13*).

Les stratégies incluent une ou plusieurs règles. Attribuez une stratégie à chaque serveur OfficeScan enregistré sur le réseau en mode épidémie et en mode normal (voir *Épidémies de risques liés à la sécurité à la page 6-98* pour obtenir de plus amples informations sur les différents modes du réseau).

Si l'état de sécurité du client OfficeScan correspond aux critères d'une règle appartenant à la stratégie, le client OfficeScan exécute les actions configurées dans la règle. Toutefois, si l'état de sécurité du client OfficeScan ne correspond pas à tout ou partie des critères de règles associés à la stratégie, vous pouvez configurer des actions par défaut dans la stratégie que le client OfficeScan et le serveur devront exécuter (consultez *Actions du client OfficeScan et du serveur Policy Server à la page 15-13*).

Conseil

Si vous souhaitez que certains clients OfficeScan d'un domaine OfficeScan disposent de stratégies de mode épidémie et de mode normal différentes de celles des autres clients OfficeScan du même domaine, Trend Micro vous suggère de restructurer les domaines en regroupant les clients OfficeScan présentant les mêmes configurations (consultez *Domaines OfficeScan à la page 2-44*).

Création des règles

Les règles comprennent des critères d'état de sécurité, des réponses par défaut associées aux clients OfficeScan et des actions à exécuter par les clients OfficeScan et le serveur Policy Server.

Critères d'état de sécurité

Les règles comprennent les critères d'état de sécurité suivants :

- **État de l'ordinateur client** : si l'ordinateur client OfficeScan est en cours d'amorçage ou pas
- **État du scan en temps réel du client** : si le scan en temps réel est activé ou désactivé
- **Actualité de la version du moteur de scan du client** : si le Moteur de scan antivirus est à jour

- **État du fichier de signatures de virus du client** : degré de mise à jour du fichier de signatures de virus. Le serveur Policy Server détermine ce point en vérifiant l'un des éléments suivants :
  - si le fichier de signatures de virus est antérieur de plusieurs versions à la version du serveur Policy Server.
  - si le fichier de signatures de virus a été mis à disposition plusieurs jours avant la validation.

Réponses par défaut des règles

Les réponses vous aident à connaître l'état des clients OfficeScan du réseau lors de la validation des clients OfficeScan. Elles apparaissent dans les journaux de validation du client du serveur Policy Server et correspondent à des jetons d'état. Vous avez le choix entre les réponses par défaut suivantes :

- **Sain** : L'ordinateur client OfficeScan est conforme aux stratégies de sécurité et n'est pas infecté.
- **Vérification** : Le client OfficeScan doit mettre à jour ses composants antivirus.
- **Infecté** : L'ordinateur client OfficeScan est infecté ou présente un risque d'infection.
- **Transition** : L'ordinateur client OfficeScan est en cours d'amorçage.
- **Quarantaine** : L'ordinateur client OfficeScan présente un risque élevé d'infection et doit être mis en quarantaine.
- **Inconnu** : Autre état

Remarque

vous ne pouvez ni ajouter, ni supprimer, ni modifier les réponses.

Actions du client OfficeScan et du serveur Policy Server

Si l'état de sécurité du client OfficeScan correspond aux critères des règles, le serveur Policy Server peut créer une entrée dans un journal de validation client du serveur Policy Server (pour plus d'informations sur ce sujet, consultez *Journaux de validation du client à la page 15-47*).

Si l'état de sécurité du client OfficeScan correspond aux critères des règles, le client OfficeScan peut exécuter les actions suivantes°:

- Activer le scan en temps réel du client afin que le client OfficeScan puisse scanner tous les fichiers ouverts et enregistrés (voir *Scan en temps réel à la page 6-15* pour obtenir de plus amples informations)
- Mettre à jour tous les composants OfficeScan (voir *Composants et programmes OfficeScan à la page 5-2* pour obtenir de plus amples informations)
- Scanner le client OfficeScan (Scan immédiat) après l'activation du scan en temps réel ou après une mise à jour
- Afficher un message de notification sur l'ordinateur client OfficeScan

Règles par défaut

Le serveur Policy Server met à votre disposition des règles par défaut pour vous aider à configurer vos paramètres. Les règles couvrent les actions et les situations de sécurité courantes et recommandées. Les règles suivantes sont disponibles par défaut :

TABLEAU 15-3. Règles par défaut

NOM DE LA RÈGLE	CRITÈRES CORRESPONDANTS	RÉPONSE EN CAS DE CORRESPONDANCE DES CRITÈRES	ACTION DU SERVEUR	ACTION DU CLIENT OFFICESCAN
Sain	L'état du scan en temps réel est activé, le moteur de scan antivirus et le fichier de signatures de virus sont à jour.	Sain	Aucune	Aucune

Nom de la règle	Critères correspondants	Réponse en cas de correspondance des critères	Action du serveur	Action du client OfficeScan
Vérification	La version du fichier de signatures de virus du client est au moins antérieure d'une version à celle du serveur OfficeScan sur lequel le client OfficeScan est enregistré.	Vérification	Créer une entrée dans le journal de validation du client	• Mettre à jour les composants • Exécuter un nettoyage immédiat automatique sur le client OfficeScan après l'activation du scan en temps réel ou après une mise à jour • Afficher le message de notification sur l'ordinateur client OfficeScan **Conseil** Si vous utilisez cette règle, optez pour le déploiement automatique. Cette opération permet de s'assurer que les clients OfficeScan reçoivent le fichier de signatures de virus le plus récent immédiatement après le téléchargement des nouveaux composants par le serveur OfficeScan.

Nom de la règle	Critères correspondants	Réponse en cas de correspondance des critères	Action du serveur	Action du client OfficeScan
Transition	L'ordinateur client OfficeScan est en cours d'amorçage.	Transition	Aucune	Aucune
Quarantaine	La version du fichier de signatures de virus du client est au moins antérieure de cinq versions à celle du serveur OfficeScan sur lequel le client OfficeScan est enregistré.	Quarantaine	Créer une entrée dans le journal de validation du client	• Mettre à jour les composants • Exécuter un nettoyage immédiat automatique et un scan immédiat sur le client OfficeScan après l'activation du scan en temps réel ou après une mise à jour • Afficher le message de notification sur l'ordinateur client OfficeScan
Non protégé	L'état du scan en temps réel est désactivé.	Infecté	Créer une entrée dans le journal de validation du client	• Activer le scan du client OfficeScan en temps réel • Afficher le message de notification sur l'ordinateur client OfficeScan

Création des stratégies

Les stratégies comprennent un nombre indéterminé de règles, ainsi que des réponses et des actions par défaut.

- **Application des règles**

Le serveur Policy Server applique les règles dans un ordre donné, ce qui permet de leur attribuer des priorités. Changez l'ordre des règles, ajoutez de nouvelles règles et supprimez les règles existantes d'une stratégie.

- **Réponses par défaut des stratégies**

  Comme pour les règles, les stratégies possèdent des réponses par défaut vous permettant de connaître l'état des clients OfficeScan du réseau lors de la validation des clients. Cependant, les réponses par défaut ne sont associées aux clients que lorsque l'état de sécurité de ceux-ci ne correspond PAS aux règles de la stratégie.

  Les réponses des stratégies et des règles sont identiques (voir *Réponses par défaut des règles à la page 15-13* pour obtenir la liste des réponses).

- **Actions du client OfficeScan et du serveur Policy Server**

  Le serveur Policy Server applique les règles aux clients en confrontant les informations relatives à l'état du client OfficeScan à chacune des règles associées à une stratégie. Les règles sont appliquées de manière descendante en fonction des règles utilisées, spécifiées dans la console Web. Si l'état du client OfficeScan correspond à l'une des règles, l'action correspondant à la règle est déployée sur le client OfficeScan. Si aucune règle ne correspond, la règle par défaut s'applique et l'action correspondant à la règle par défaut est déployée sur les clients.

  La stratégie par défaut en mode épidémie évalue les clients OfficeScan à l'aide de la règle «°Sain°». Elle oblige tous les clients OfficeScan ne correspondant à cette règle à exécuter immédiatement les actions correspondant à la réponse «°Infecté°».

  La stratégie par défaut en mode normal évalue les clients OfficeScan à l'aide de toutes les règles autres que «°Sain°» (Transition, Non protégé, Quarantaine, Vérification). Elle classe tous les clients OfficeScan ne correspondant à aucune de ces règles comme clients «°sains°» et applique les actions correspondant à la règle «°Sain°».

Stratégies par défaut

Le serveur Policy Server met à votre disposition des stratégies par défaut pour vous aider à configurer vos paramètres. Deux stratégies sont disponibles : une pour le mode normal et une autre pour le mode épidémie.

TABLEAU 15-4. Stratégies par défaut

NOM DE LA STRATÉGIE	DESCRIPTION
Stratégie par défaut en mode normal	• Règles par défaut associées à cette stratégie : Transition, Non protégé, Quarantaine et Vérification • Réponse si aucune des règles ne correspond : Sain • Action du serveur : Aucune • Action du client OfficeScan : Aucune

Stratégie par défaut en mode épidémie	• Règles par défaut associées à cette stratégie : Sain
	• Réponse si aucune des règles ne correspond : Infecté
	• Action du serveur : Créer une entrée dans le journal de validation du client
	• Action du client OfficeScan :
	  • Activer le scan du client en temps réel
	  • Mettre à jour les composants
	  • Exécuter un scan immédiat sur le client OfficeScan après l'activation du scan en temps réel ou après une mise à jour
	  • Afficher un message de notification sur l'ordinateur client OfficeScan

Synchronisation

Synchronisez régulièrement le serveur Policy Server avec les serveurs OfficeScan enregistrés afin de maintenir à jour les versions de fichier de signatures de virus et de moteur de scan antivirus, ainsi que l'état de l'épidémie du serveur (mode normal ou mode épidémie) à la fois sur le serveur Policy Server et sur le serveur OfficeScan. Pour effectuer la synchronisation, procédez comme suit :

- **Manuellement** : Exécutez la synchronisation à tout moment dans l'écran Résumé (consultez *Résumé des informations d'un serveur Policy Server à la page 15-44*).

- **Par programmation** : Configurer un programme de synchronisation (consultez *Tâches administratives à la page 15-47*).

Certificats

La technologie Cisco NAC fait appel aux certificats numériques suivants afin d'établir une bonne communication entre les divers composants :

TABLEAU 15-5. Certificats Cisco NAC

CERTIFICAT	DESCRIPTION
certificat ACS	Établit une communication fiable entre le serveur ACS et le serveur de l'autorité de certification (CA). Le serveur de l'autorité de certification signe le certificat ACS avant que vous ne l'enregistriez sur le serveur ACS.
certificat CA	Authentifie les clients OfficeScan auprès du serveur Cisco ACS. Le serveur OfficeScan déploie le certificat CA sur le serveur ACS et sur les clients OfficeScan (fourni avec le pack Cisco Trust Agent).
Certificat SSL du serveur Policy Server	Sécurise la communication HTTPS entre le serveur Policy Server et le serveur ACS. Le certificat SSL du serveur Policy Server est automatiquement généré par le serveur Policy Server, pendant l'installation de ce dernier. le certificat SSL du serveur Policy Server est facultatif. Utilisez-le cependant pour vous assurer que seules les données chiffrées sont échangées entre le serveur Policy Server et le serveur ACS.

La figure ci-dessous illustre les étapes de la création et du déploiement des certificats ACS et CA :

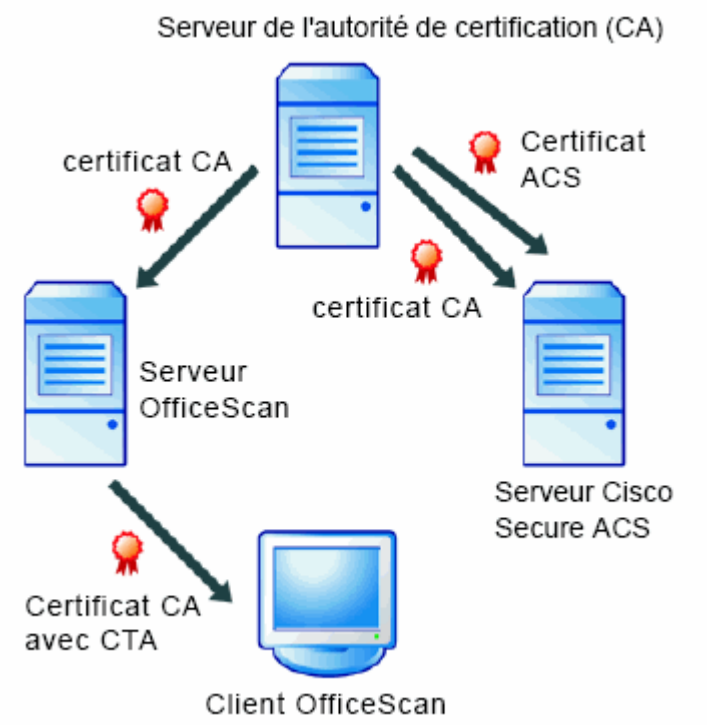


FIGURE 15-4. Création et déploiement des certificats ACS et CA

1. Après l'émission par le serveur ACS d'une demande de signature de certificat au serveur CA, ce dernier émet un certificat appelé Certificat ACS. Le certificat ACS est ensuite installé sur le serveur ACS. Voir la *Inscription du serveur Cisco Secure ACS à la page 15-27* pour plus d'informations.
2. Un certificat CA est exporté depuis le serveur CA et installé sur le serveur ACS. Voir *Installation du certificat CA à la page 15-27* pour obtenir des instructions détaillées.
3. Une copie de ce même certificat CA est enregistrée sur le serveur OfficeScan.

4. Le serveur OfficeScan déploie le certificat CA sur les clients OfficeScan avec CTA. Voir *Déploiement de Cisco Trust Agent à la page 15-30* pour obtenir des instructions détaillées.

Le certificat CA

Les clients OfficeScan dotés des installations CTA procèdent à une authentification auprès du serveur ACS avant de communiquer l'état de sécurité du client. Il existe plusieurs méthodes d'authentification (consultez la documentation du serveur Cisco Secure ACS pour obtenir des informations détaillées). Vous avez par exemple peut être déjà activé l'authentification de l'ordinateur pour le serveur Cisco Secure ACS à l'aide de Windows Active Directory, que vous pouvez configurer afin de produire automatiquement un certificat client pour l'utilisateur final lorsqu'un nouvel ordinateur est ajouté dans Active Directory. Pour obtenir des instructions à ce sujet, consultez la base de connaissances Microsoft, article 313407, HOW TO: Créer des demandes de certificat automatique avec stratégie de groupe sous Windows.

Pour les utilisateurs qui disposent de leur propre serveur d'autorité de certification (CA), mais dont les clients utilisateurs finaux ne possèdent pas encore de certificats, OfficeScan prévoit un mécanisme destiné à distribuer un certificat racine aux clients OfficeScan. Distribuez le certificat pendant l'installation d'OfficeScan ou à partir de la console Web d'OfficeScan. OfficeScan distribue le certificat lorsqu'il déploie Cisco Trust Agent sur les clients OfficeScan (consultez *Déploiement de Cisco Trust Agent à la page 15-30*).

Remarque

Si vous avez déjà acquis un certificat auprès d'une autorité de certification ou si vous avez produit et distribué vos propres certificats aux clients utilisateurs finaux OfficeScan, il est inutile de recommencer.

Avant de distribuer le certificat aux clients OfficeScan, enregistrez le serveur ACS auprès du serveur CA et préparez le certificat (pour plus d'informations, consultez *Inscription du serveur Cisco Secure ACS à la page 15-27*).

Configuration minimale requise pour le serveur Policy Server

Avant de procéder à l'installation du serveur Policy Server, vérifiez que l'ordinateur bénéficie de la configuration nécessaire°:

TABLEAU 15-6. Configuration minimale requise pour le serveur Policy Server

SPÉCIFICATIONS LOGICIELLES/ MATÉRIELLES	CONFIGURATION REQUISE
Système d'exploitation	• Windows 2000 Professional avec Service Pack 4 • Windows 2000 Server avec Service Pack 4 • Windows 2000 Advanced Server Service Pack 4 • Windows XP Professionnel avec Service Pack 3 ou supérieur, 32 bits et 64 bits • Windows Server 2003 (éditions Standard et Enterprise) avec Service Pack 2 ou supérieur, versions 32 bits et 64 bits
Matériel	• Processeur Intel Pentium II 300 MHz ou équivalent • 128 Mo de mémoire vive • 300 Mo d'espace disque disponible • Écran avec résolution 800 x 600 pixels, 256 couleurs minimum
Serveur Web	• Microsoft Internet Information Server (IIS) version 5.0 ou 6.0 • Serveur Web Apache 2.0 ou supérieur (pour Windows 2000/XP/Server 2003 uniquement)

SPÉCIFICATIONS LOGICIELLES/ MATÉRIELLES	CONFIGURATION REQUISE
Console Web	Pour utiliser la console Web du serveur OfficeScan, il vous faut : • Processeur Intel Pentium 133MHz ou équivalent • 64 Mo de mémoire vive • 30 Mo d'espace disque disponible • Écran avec résolution 800 x 600 pixels, 256 couleurs minimum • Microsoft Internet Explorer 5.5 ou supérieur

Configuration requise pour Cisco Trust Agent (CTA)

Avant de procéder au déploiement de l'agent Cisco Trust Agent sur les ordinateurs clients, vérifiez si les ordinateurs bénéficient de la configuration nécessaire°:

Remarque

Cisco Trust Agent ne prend pas en charge l'adressage IPv6. Vous ne pouvez pas déployer l'agent dans des points finaux IPv6 purs.

TABLEAU 15-7. Configuration requise pour Cisco Trust Agent (CTA)

SPÉCIFICATIONS LOGICIELLES/ MATÉRIELLES	CONFIGURATION REQUISE
Système d'exploitation	• Windows 2000 Professionnel et Server avec Service Pack 4 • Windows XP Professionnel avec Service Pack 3 ou supérieur, 32 bits • Windows Server 2003 (éditions Standard et Enterprise) avec Service Pack 2 ou supérieur, 32 bits

SPÉCIFICATIONS LOGICIELLES/ MATÉRIELLES	CONFIGURATION REQUISE
Matériel	• Un ou plusieurs processeurs Intel Pentium 200 MHz • 128 Mo de mémoire vive pour Windows 2000 • 256 Mo de mémoire vive pour Windows XP et Windows Server 2003 • 5 Mo d'espace disque disponible (20 Mo recommandés)
Autres	• Windows Installer 2.0 ou supérieur

Plates-formes prises en charge et configuration requise

Les plates-formes suivantes prennent en charge la fonction Cisco NAC°:

TABLEAU 15-8. Plates-formes prises en charge et configuration requise

PLATES-FORMES PRISES EN CHARGE	MODÈLES	IMAGES IOS	MÉMOIRE MINIMUM/ FLASH
Routeurs			
Cisco 830, 870 series	831, 836, 837	IOS 12.3(8) ou ultérieur	48 Mo/8 Mo
Cisco 1700 series	1701, 1711, 1712, 1721, 1751, 1751-V, 1760	IOS 12.3(8) ou ultérieur	64 Mo/16 Mo
Cisco 1800 series	1841	IOS 12.3(8) ou ultérieur	128 Mo/32 Mo
Cisco 2600 series	2600XM, 2691	IOS 12.3(8) ou ultérieur	96 Mo/32 Mo
Cisco 2800 series	2801, 2811, 2821, 2851	IOS 12.3(8) ou ultérieur	128 Mo/64 Mo

Plates-formes prises en charge	Modèles	Images IOS	Mémoire minimum/ Flash
Cisco 3600 series	3640/3640A, 3660-ENT series	IOS 12.3(8) ou ultérieur	48 Mo/16 Mo
Cisco 3700 series	3745, 3725	IOS 12.3(8) ou ultérieur	128 Mo/32 Mo
Cisco 3800 series	3845, 3825	IOS 12.3(8) ou ultérieur	256 Mo/64 Mo
Cisco 7200 series	720x, 75xx	IOS 12.3(8) ou ultérieur	128 Mo/48 Mo
Concentrateurs RPV			
Cisco VPN 3000 Series	3005 - 3080	V4.7 ou ultérieur	N/A
Commutateurs			
Cisco Catalyst 2900	2950, 2970	IOS 12.1(22)EA5	N/A
Cisco Catalyst 3x00	3550, 3560, 3750	IOS 12.2(25)SEC	N/A
Cisco Catalyst 4x00	Supervisor 2+ ou supérieur	IOS 12.2(25)EWA	N/A
Cisco Catalyst 6500	6503, 6509, Supervisor 2 ou supérieur	CatOS 8.5 ou ultérieur	Sup2 - 128 Mo, Sup32 - 256 Mo, Sup720 - 512 Mo
Points d'accès sans fil			
Cisco AP1200 Series	1230	N/A	N/A

Déploiement de Policy Server for NAC

Les procédures suivantes ne sont fournies qu'à titre de référence et sont susceptibles de varier en fonction des mises à jour ou de la présence d'interfaces Microsoft et/ou Cisco.

Avant d'effectuer l'une des tâches, vérifiez que le ou les périphériques d'accès réseau situés sur le réseau prennent en charge Cisco NAC (consultez *Plates-formes prises en charge et configuration requise à la page 15-24*). Reportez-vous à la documentation de votre périphérique pour les instructions d'installation et de configuration. Installez également le serveur ACS sur le réseau. Reportez-vous à la documentation relative au serveur Cisco Secure ACS pour obtenir les instructions.

1. Installez le serveur OfficeScan sur le réseau (voir le *Guide d'installation et de mise à niveau*).
2. Installez le programme client OfficeScan sur tous les clients dont le serveur Policy Server doit évaluer la protection.
3. Inscrivez le serveur Cisco Secure ACS. Établissez une relation de confiance entre le serveur ACS et un serveur d'autorité de certificat (CA) par l'émission par le serveur ACS d'une demande de signature de certificat. Enregistrez ensuite le certificat CA signé (appelé certificat ACS) sur le serveur ACS (pour plus d'informations, consultez *Inscription du serveur Cisco Secure ACS à la page 15-27*).
4. Exportez le certificat CA vers le serveur ACS et enregistrez une copie de ce certificat sur le serveur OfficeScan. Cette étape est nécessaire uniquement si vous n'avez pas déployé de certificat sur les clients et le serveur ACS (voir *Installation du certificat CA à la page 15-27*).
5. Déployez l'agent Cisco Trust Agent et le certificat CA chez tous les clients OfficeScan pour que ceux-ci puissent soumettre des informations sur l'état de sécurité au serveur Policy Server (voir *Déploiement de Cisco Trust Agent à la page 15-30*).
6. Installez le serveur Policy Server pour Cisco NAC afin qu'il traite les demandes depuis le serveur ACS (voir *Installation du serveur Policy Server for Cisco NAC à la page 15-35*).
7. Exportez un certificat SSL depuis le serveur Policy Server vers le serveur Cisco ACS pour établir des communications SSL sécurisées entre les deux serveurs (voir *Installation du serveur Policy Server for Cisco NAC à la page 15-35*).
8. Configurez le serveur ACS pour transmettre des requêtes de validation d'état au serveur Policy Server (voir *Configuration du serveur ACS à la page 15-41*).
9. Configuration du serveur Policy Server for Cisco NAC. Créez et modifiez les règles et stratégies du serveur Policy Server pour mettre en application la stratégie de

sécurité de votre entreprise sur les clients OfficeScan (voir *Configuration du serveur Policy Server for Cisco NAC à la page 15-42*).

Inscription du serveur Cisco Secure ACS

Inscrivez le serveur Cisco Secure ACS auprès du serveur de l'autorité de certification (CA) afin d'établir une relation de confiance entre les deux serveurs. la procédure suivante est destinée aux utilisateurs exécutant un serveur d'autorité de certification Windows afin de gérer les certificats sur le réseau. Reportez-vous à la documentation du fournisseur si vous utilisez un service ou une application CA différente, puis consultez la documentation du serveur ACS pour obtenir les instructions sur la procédure d'inscription d'un certificat.

Installation du certificat CA

Le client OfficeScan s'authentifie auprès du serveur ACS avant d'envoyer les données de l'état de sécurité. Le certificat CA est nécessaire pour que cette authentification puisse avoir lieu. Commencez par exporter le certificat CA depuis le serveur CA vers les serveurs ACS et OfficeScan puis créez le pack de déploiement de l'agent CTA. Ce pack contient le certificat CA (voir *Le certificat CA à la page 15-21* et *Déploiement de Cisco Trust Agent à la page 15-30*).

Exécutez les opérations suivantes pour exporter et installer le certificat CA°:

- Exportez le certificat CA depuis le serveur de l'autorité de certificat
- Installez-le sur le serveur Cisco Secure ACS
- Enregistrez une copie sur le serveur OfficeScan

Remarque

la procédure suivante est destinée aux utilisateurs exécutant un serveur d'autorité de certification Windows afin de gérer les certificats sur le réseau. Si vous utilisez une application ou un service d'autorité de certification différent, consultez la documentation livrée par le fournisseur.

Exportation et installation du certificat CA en vue de la distribution

Tâche

1. Exportez le certificat depuis le serveur de l'autorité de certification (CA) :

   a. Sur le serveur CA, cliquez sur **Démarrer** > **Exécuter**.

      L'écran Exécuter apparaît.

   b. Saisissez `mmc` dans le champ **Ouvrir**.

      Un nouvel écran de console d'administration s'ouvre.

   c. Cliquez sur **Fichier** > **Ajouter/Supprimer un composant logiciel enfichable**.

      L'écran **Ajouter/Supprimer un composant logiciel enfichable** apparaît.

   d. Cliquez sur **Certificats** puis sur **Ajouter**.

      L'écran **Composant logiciel enfichable Certificats** apparaît.

   e. Cliquez sur **Compte d'ordinateur** puis sur **Suivant**.

      L'écran **Select Computer** apparaît.

   f. Cliquez sur **Ordinateur local** puis sur **Terminer**.

   g. Pour fermer l'écran **Ajout d'un composant logiciel enfichable autonome**, cliquez sur **Fermer**.

   h. Cliquez sur **OK** pour fermer l'écran **Ajouter/Supprimer un composant logiciel enfichable**.

   i. Dans l'arborescence de la console, cliquez sur **Certificats** > **Racine de confiance** > **Certificats**.

   j. Dans la liste, sélectionnez le certificat que vous distribuerez aux clients et le serveur ACS.

   k. Cliquez sur **Action** > **Toutes les tâches** > **Exporter...**.

      L'**Assistant Exportation de certificat** s'ouvre.

l. Cliquez sur **Suivant**.

m. Cliquez sur **Binaire codé DER X.509** puis sur **Suivant**.

n. Saisissez un nom de fichier et naviguez vers un répertoire dans lequel le certificat sera exporté.

o. Cliquez sur **Suivant**.

p. Cliquez sur **Terminer**.

Une fenêtre de confirmation apparaît.

q. Cliquez sur **OK**.

2. Installez le certificat sur le serveur Cisco Secure ACS.

a. Cliquez sur **Configuration du système** > **Installation du certificat ACS** > **Installation de l'autorité de certification ACS**.

b. Saisissez le chemin d'accès complet et le nom du fichier du certificat dans le champ **Fichier de certificats d'Autorité de certification**.

c. Cliquez sur **Envoyer**. Cisco Secure ACS vous invite à redémarrer le service.

d. Cliquez sur **Configuration du système** > **Contrôle du service**.

e. Cliquez sur **Redémarrer**. Cisco Secure ACS redémarre.

f. Cliquez sur **Configuration du système** > **Gestion de certificat ACS** > **Modifier la liste de certificats de confiance**. L'écran **Edit Certificate Trust List** apparaît.

g. Cochez la case correspondant au certificat que vous avez importé lors de l'étape b puis cliquez sur **Envoyer**. Cisco Secure ACS vous invite à redémarrer le service.

h. Cliquez sur **Configuration du système** > **Contrôle du service**.

i. Cliquez sur **Redémarrer**. Cisco Secure ACS redémarre.

3. Copiez le certificat (fichier .cer) sur l'ordinateur du serveur OfficeScan, pour le déployer sur le client avec le CTA (voir pour obtenir de plus amples informations).

Remarque

Enregistrez le certificat sur un lecteur local ; les lecteurs mappés ne sont pas acceptés.

Déploiement de Cisco Trust Agent

Cisco Trust Agent (CTA), programme hébergé par le serveur OfficeScan et installé sur les clients, permet au client OfficeScan de signaler des informations antivirus vers Cisco ACS.

Remarque

Cisco Trust Agent ne prend pas en charge l'adressage IPv6. Vous ne pouvez pas déployer l'agent dans des points finaux IPv6 purs.

Déploiement de CTA pendant l'installation du serveur OfficeScan

Si vous avez déjà préparé un certificat CA avant d'installer le serveur OfficeScan, déployez l'agent CTA pendant l'installation du serveur OfficeScan. L'option de déploiement de l'agent CTA s'affiche dans l'écran **Installation d'autres programmes OfficeScan** du programme d'installation. Pour obtenir des instructions sur l'installation du serveur OfficeScan, consultez le *Guide d'installation et de mise à niveau*.

Tâche

1. Dans l'écran **Installation d'autres programmes OfficeScan**, sélectionnez **Cisco Trust Agent for Cisco NAC**.
2. Si vous avez déjà distribué des certificats aux clients utilisateurs finaux de Cisco Secure NAC, cliquez sur **Suivant**. Sinon, procédez de la manière suivante pour distribuer les certificats :
   a. Cliquez sur **Importer le certificat**.
   b. Localisez et sélectionnez le fichier de certificat préparé, puis cliquez sur **Ok**.

      Pour obtenir des instructions sur la préparation d'un fichier de certificat, consultez *Installation du certificat CA à la page 15-27*.

c. Cliquez sur **Suivant**.

3. Poursuivez l'installation du serveur OfficeScan.

Déploiement de CTA à partir d'OfficeScan Web Console

Si vous n'avez pas sélectionné l'option d'installation/de mise à jour de CTA pendant l'installation du serveur, vous pouvez le faire depuis la console Web. Avant d'installer/de mettre à niveau CTA, déployez le certificat client sur les clients OfficeScan.

Remarque

Le serveur de l'autorité de certification (CA) génère le fichier de certificat client. Demandez un fichier de certificat à votre revendeur Trend Micro.

Une fois prêt pour l'installation/la mise à niveau, vérifiez la version de CTA à installer dans **Cisco NAC** > **Gestion des agents**, puis installez CTA sur les clients OfficeScan avec **Cisco NAC** > **Déploiement de l'agent**. L'écran Déploiement de l'agent permet également de désinstaller CTA.

Installez le client Windows Installer 2.0 pour NT 4.0 sur les clients OfficeScan exécutant Windows 2000/XP avant de déployer l'agent.

Importation du certificat client

Le certificat client (ou CA) authentifie les clients utilisateurs finaux d'OfficeScan avec le serveur Cisco ACS. Le serveur OfficeScan déploie le certificat CA sur les clients OfficeScan avec Cisco Trust Agent (CTA). Vous devez, par conséquent importer le certificat à destination du serveur OfficeScan avant de déployer CTA.

Tâche

1. Ouvrez la console Web du serveur OfficeScan et cliquez sur **Cisco NAC** > **Certificat client**.

2. Saisissez le chemin d'accès au certificat.

3. Saisissez le chemin d'accès complet et le nom du fichier du certificat CA enregistré sur le serveur (par exemple : `C:\CiscoNAC\certificate.cer`). Pour obtenir

des instructions sur la préparation d'un certificat CA, consultez *Installation du certificat CA à la page 15-27*.

4. Cliquez sur **Importer**.

   Pour effacer le contenu d'un champ, cliquez sur **Réinitialiser**.

Version de Cisco Trust Agent

Avant l'installation de CTA sur les clients, vérifiez la version de CTA à installer (Cisco Trust Agent ou Cisco Trust Agent Supplicant). La seule différence entre ces deux versions réside dans le fait que le pack Supplicant permet une authentification à deux couches pour l'ordinateur et l'utilisateur final.

Si vous disposez de la version 4.0 ou supérieure de Cisco NAC Access Control Server (ACS), procédez à une mise à niveau de Cisco Trust Agent sur les clients vers la version 2.0 ou ultérieure.

Vérification de la version de CTA

Tâche

1. Ouvrez la console Web du serveur OfficeScan et cliquez sur **Cisco NAC** > **Gestion des agents**.
2. Cliquez sur **Utiliser <Version CTA>**.

   Le serveur OfficeScan commence à utiliser la nouvelle version.

Remplacement manuel du pack de CTA

Remplacez manuellement le pack CTA sur le serveur OfficeScan si vous souhaitez utiliser une version particulière.

Tâche

1. Dans la version CTA que vous souhaitez utiliser, copiez le fichier CTA `.msi` dans l'un des dossiers suivants :

- <*Dossier d'installation du serveur*>\PCCSRV\Admin\Utility\CTA\CTA-Package
- <Dossier d'installation du serveur>\PCCSRV\Admin\Utility\CTA\ CTA-Supplicant-Package

2. Copiez les fichiers suivants dans <Dossier d'installation du serveur>\PCCSRV\Admin\Utility\CTA\PosturePlugin : TmabPP.dll, tmabpp.inf et TmAbPpAct.exe.
3. Dans la console Web, accédez à **Cisco NAC** > **Gestion des agents** et cliquez sur **Utiliser <version CTA>**.

Après la mise à niveau de l'agent, les fichiers seront compressés dans PostureAgent.zip en tant que pack de déploiement CTA sous <Dossier d'installation du serveur>\PCCSRV\download\Product.

Déploiement de Cisco Trust Agent

Déployez Cisco Trust Agent pour permettre au client OfficeScan de transmettre les informations sur les virus à Cisco ACS.

Tâche

1. Accédez à **Cisco NAC** > **Déploiement de l'agent**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.
3. Clique sur **Déployer l'agent**.
4. Si vous n'avez pas accepté les conditions du contrat de licence Cisco lors de l'installation du serveur OfficeScan, les informations sur la licence s'affichent. Lisez attentivement le contrat de licence puis cliquez sur **Oui** pour confirmer votre acceptation.
5. Sélectionnez **Installer/Mettre à niveau Cisco Trust Agent**.
6. (Facultatif) Sélectionnez **Désinstaller Cisco Trust Agent lors de la désinstallation du client OfficeScan**.

Remarque

Utilisez également cet écran pour la désinstallation ou la conservation de l'état de CTA sur les clients.

Conserver l'état de CTA signifie empêcher une installation d'écraser le CTA existant. Sauf si vous procédez à une mise à jour ou si vous êtes sûr(e) que vous n'avez jamais installé de CTA sur l'un des clients sélectionnés, utilisez cette option, sinon le serveur réinstallera le CTA et vos paramètres seront perdus.

7. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Remarque

Si le client OfficeScan sur lequel l'agent est déployé n'est pas connecté lorsque vous cliquez sur **Installer Cisco Trust Agent**, OfficeScan remplit automatiquement la tâche demandée lorsque le client OfficeScan se connecte.

Vérification de l'installation de l'agent Cisco Trust Agent

Lorsque vous avez déployé l'agent CTA sur les clients OfficeScan, vérifiez que l'installation a bien réussi en consultant l'arborescence des clients. L'arborescence client contient une colonne intitulée **Programme CTA**, qui s'affiche dans **Mettre à jour**, **Afficher tout**ou **Antivirus**. Les installations réussies de l'agent CTA contiennent un numéro de version du programme CTA.

Vérifiez également que les processus suivants s'exécutent sur l'ordinateur client :

- `ctapsd.exe`

- `ctaEoU.exe`
- `ctatransapt.exe`
- `ctalogd.exe`

Installation du serveur Policy Server for Cisco NAC

Il existe deux façons d'installer le serveur Policy Server :

- Le programme d'installation du serveur Policy Server sur le DVD version Entreprise
- Le programme d'installation principal du serveur OfficeScan (installe à la fois le serveur OfficeScan et le serveur Policy Server sur un même ordinateur)

Remarque

Le programme d'installation principal installe à la fois le serveur OfficeScan et la console Web du serveur Policy Server sur un serveur Web IIS ou Apache. Si le programme d'installation ne trouve pas de serveur Apache sur le système ou si la version du serveur Apache installée ne correspond pas au minimum à la version 2.0, il installe automatiquement Apache version 2.0.

Le serveur ACS, le serveur Policy Server et le serveur OfficeScan doivent se trouver sur le même segment de réseau pour garantir une communication efficace.

Avant d'installer le serveur Web Apache, consultez le site Web Apache pour obtenir les informations les plus récentes sur les mises à niveau, les patchs et les problèmes de sécurité à l'adresse suivante :

http://www.apache.org

Installation du serveur Policy Server à l'aide du programme d'installation du serveur Policy Server

---

Tâche

1. Connectez-vous à l'ordinateur sur lequel vous souhaitez installer Policy Server for Cisco NAC.

2. Placez le logiciel d'installation de Policy Server for Cisco NAC qui se trouve sur le CD version Entreprise.
3. Double-cliquez sur `setup.exe` pour exécuter le programme d'installation.
4. Suivez les instructions d'installation.

Vous pouvez aussi installer le serveur Policy Server sur le même ordinateur que le serveur OfficeScan.

Installation du serveur Policy Server for Cisco NAC à partir du programme d'installation principal du serveur OfficeScan

---

Tâche

1. Dans l'écran **« Installation d'autres programmes OfficeScan »** du programme d'installation principal du serveur OfficeScan, sélectionnez **Policy Server for Cisco NAC**.
2. Cliquez sur **Suivant**.
3. Poursuivez l'installation du serveur OfficeScan jusqu'à ce que l'écran **Bienvenue de Trend Micro Policy Server for Cisco NAC** s'affiche.
4. Cliquez sur **Suivant**.

   L'écran **Contrat de licence du Policy Server pour Cisco NAC** apparaît.
5. Lisez le contrat et cliquez sur **Oui** pour continuer.

   L'écran **Choisir l'emplacement de destination** apparaît.
6. Si nécessaire, modifiez l'emplacement de destination par défaut en cliquant sur **Parcourir...** et sélectionnez une nouvelle destination pour l'installation du serveur Policy Server.
7. Cliquez sur **Suivant**.

   L'écran **Serveur Web** apparaît.
8. Sélectionnez le serveur Web pour le serveur Policy Server :

- **Serveur IIS** : cliquez ici pour procéder à l'installation sur une installation de serveur Web IIS existant
- **Serveur Web Apache 2.0** : cliquez ici pour procéder à l'installation sur un serveur Web Apache 2.0.

9. Cliquez sur **Suivant**.

L'écran **Configuration du Serveur Web** apparaît.

10. Configurez les informations suivantes :

a. Si vous avez choisi d'installer le serveur Policy Server sur un serveur IIS, sélectionnez l'une des options suivantes :

- **Site Web IIS par défaut** : cliquez ici pour installer le site Web IIS en tant que site Web par défaut
- **Site Web IIS virtuel** Cliquez ici pour installer le site Web IIS en tant que site Web par défaut.

b. En regard de **Port**, saisissez un port qui sera utilisé en tant que port d'écoute du serveur.

Si le serveur Policy Server et le serveur OfficeScan se trouvent sur le même ordinateur et utilisent le même serveur Web, les numéros de ports sont les suivants :

- **Serveur Web Apache/IIS sur le site Web par défaut** : le serveur Policy Server et le serveur OfficeScan partagent le même port.
- **Tous deux sur le serveur Web IIS sur le site Web virtuel** : le port d'écoute par défaut du serveur Policy Server est le port 8081 et son port SSL est le 4344. Le port d'écoute par défaut du serveur OfficeScan est le 8080 et son port SSL est le 4343.

c. Si vous installez le serveur Policy Server sur un serveur IIS, vous pouvez utiliser Secured Socket Layer (SSL). Saisissez le numéro de port SSL et la durée de validité du certificat SSL en années (par défaut, 3 ans).

Si vous activez SSL, ce numéro de port servira de port d'écoute du serveur. L'adresse du serveur Policy Server se présente comme suit :

- `http://<nom du serveur Policy Server> :<numéro de port>`
- `https://<nom du serveur Policy Server> :<numéro de port>` (si vous avez activé SSL)

11. Cliquez sur **Suivant**.
12. Spécifiez le mot de passe de la console du serveur Policy Server, puis cliquez sur **Suivant**.
13. Spécifiez le mot de passe d'authentification du serveur ACS, puis cliquez sur **Suivant**.
14. Vérifiez les paramètres d'installation. Si les paramètres vous conviennent, cliquez sur **Suivant** pour démarrer l'installation. Sinon, cliquez sur **Précédent** pour revenir aux écrans précédents.
15. Lorsque l'installation est terminée, cliquez sur **Terminer**.

    Le programme d'installation principal poursuit le reste de l'installation du serveur OfficeScan.

Préparation du certificat SSL du serveur Policy Server

Pour établir une connexion SSL sécurisée entre le serveur ACS et le serveur Policy Server, préparez un certificat spécialement conçu pour être utilisé avec SSL. Le certificat SSL est automatiquement généré pendant l'installation.

Préparation du certificat SSL du serveur IIS Policy Server

Tâche

1. Exportez le certificat depuis Certification Store sur mmc :
   a. Sur le serveur Policy Server, cliquez sur **Démarrer** > **Exécuter**.

      L'écran Exécuter apparaît.

   b. Saisissez `mmc` dans le champ **Ouvrir**.

Un nouvel écran de console d'administration s'ouvre.

c. Cliquez sur **Console** > **Ajouter/Supprimer un composant logiciel enfichable**.

L'écran Ajouter/Supprimer un composant logiciel enfichable apparaît.

d. Cliquez sur **Ajouter**.

L'écran **Ajout de composants logiciels enfichables autonomes** apparaît.

e. Cliquez sur **Certificats** puis sur **Ajouter**.

L'écran **Composant logiciel enfichable Certificats** apparaît.

f. Cliquez sur **Compte d'ordinateur** puis sur **Suivant**.

L'écran **Select Computer** apparaît.

g. Cliquez sur **Ordinateur local** puis sur **Terminer**.

h. Pour fermer l'écran **Ajout d'un composant logiciel enfichable autonome**, cliquez sur **Fermer**.

i. Cliquez sur **OK** pour fermer l'écran **Ajouter/Supprimer un composant logiciel enfichable**.

j. Dans l'arborescence de la console, cliquez sur **Certificats (ordinateur local)** > **Racine de confiance, Autorités de certification** > **Certificats**.

k. Sélectionnez le certificat dans la liste :

Remarque

Vérifiez le certificat d'empreinte en double cliquant sur le certificat, puis en sélectionnant Propriétés. L'empreinte doit être la même que celle du certificat qui se trouve dans la console IIS.

Pour vérifier, ouvrez la console IIS et cliquez avec le bouton droit de la souris sur **site Web virtuel** ou sur **site Web par défaut** (selon le site Web sur lequel vous avez installé le serveur Policy Server), puis sélectionnez **Propriétés**. Cliquez sur **Sécurité du répertoire** puis sur **Afficher le Certificat** pour consulter les détails du certificat, y compris l'empreinte.

---

l. Cliquez sur **Action** > **Toutes les tâches** > **Exporter...**. L'**Assistant Exportation de certificat** s'ouvre.

m. Cliquez sur **Suivant**.

n. Cliquez sur **Binaire codé DER X.509** ou sur **Codé à base 64 X.509**, puis cliquez sur **Suivant**.

o. Saisissez un nom de fichier et naviguez vers un répertoire dans lequel le certificat sera exporté.

p. Cliquez sur **Suivant**.

q. Cliquez sur **Terminer**. Une fenêtre de confirmation apparaît.

r. Cliquez sur **OK**.

2. Installez le certificat sur le serveur Cisco Secure ACS.

a. Sur la console Web ACS, cliquez sur **Configuration du système** > **Installation du certificat ACS** > **Installation de l'autorité de certification ACS**.

b. Saisissez le chemin d'accès complet et le nom du fichier du certificat dans le champ **Fichier de certificats d'Autorité de certification**.

c. Cliquez sur **Envoyer**. Cisco Secure ACS vous invite à redémarrer le service.

d. Cliquez sur **Configuration du système** > **Contrôle du service**.

e. Cliquez sur **Redémarrer**. Cisco Secure ACS redémarre.

Préparation du certificat SSL du serveur Apache Policy Server

---

Tâche

1. Exportez le certificat depuis Certification Store sur mmc :

a. Obtenez le fichier certificat `server.cer`. L'endroit où se trouve le fichier dépend du serveur OfficeScan du serveur Policy Server, que vous avez installé en premier lieu :

- Si vous avez installé le serveur OfficeScan avant d'installer le serveur Policy Server, le fichier se trouve dans le répertoire suivant : <*Dossier d'installation du serveur*>`\PCCSRV\Private\certificate`
- Si vous avez installé le serveur Policy Server avant d'installer le serveur OfficeScan, le fichier se trouve dans le répertoire suivant : `<Dossier d'installation du serveur>\PolicyServer\Private \certificate`

b. Copiez le fichier de certificat sur le serveur ACS.

2. Installez le certificat sur le serveur Cisco Secure ACS.

a. Sur la console Web ACS, cliquez sur **Configuration du système** > **Installation du certificat ACS** > **Installation de l'autorité de certification ACS**.

b. Saisissez le chemin d'accès complet et le nom du fichier du certificat dans le champ **Fichier de certificats d'Autorité de certification**.

c. Cliquez sur **Envoyer**.

Cisco Secure ACS vous invite à redémarrer le service.

d. Cliquez sur **Configuration du système** > **Contrôle du service**.

e. Cliquez sur **Redémarrer**.

Cisco Secure ACS redémarre.

Configuration du serveur ACS

Pour permettre à Cisco Secure ACS de transmettre des demandes d'authentification au serveur Policy Server for Cisco NAC, ajoutez le serveur Policy Server for Cisco NAC dans External Policies pour que la base de données de l'utilisateur externe utilise l'authentification. Consultez la documentation du serveur ACS pour obtenir des instructions sur l'ajout du serveur Policy Server à une nouvelle stratégie externe.

Remarque

Configurez le serveur ACS pour qu'il exécute des tâches telles que le blocage de l'accès des clients au réseau. Ces fonctions ACS ne font pas partie du champ d'action de Trend Micro Policy Server for Cisco NAC et ne sont donc pas reprises dans cette documentation. Pour obtenir des informations détaillées sur la configuration des autres fonctions ACS, consultez la documentation ACS.

Configuration du serveur Policy Server for Cisco NAC

Lorsque OfficeScan et le serveur Policy Server sont installés et que le client OfficeScan et l'agent Cisco Trust Agent sont déployés, configurez le serveur Policy Server for Cisco NAC. Pour configurer un serveur Policy Server, accédez à la console Web du serveur Policy Server via la console Web OfficeScan en accédant à **Cisco NAC** > **Serveurs Policy Server**, puis en cliquant sur le lien Policy Server.

Ce chapitre décrit les aspects suivants de la configuration du serveur Policy Server :

- *Configuration du serveur Policy Server depuis OfficeScan à la page 15-43* décrit comment gérer les serveurs Policy Server sur la console Web d'OfficeScan.
- *Résumé des informations d'un serveur Policy Server à la page 15-44* vous montre comment obtenir un aperçu des serveurs Policy Server du réseau.
- *Enregistrement du serveur Policy Server à la page 15-45* est la première étape de la configuration des serveurs Policy Server.
- *règles à la page 15-46* vous montre comment créer et modifier des règles qui contiennent des stratégies.
- *Stratégies à la page 15-46* vous montre comment créer et modifier des stratégies qui déterminent comment le serveur Policy Server mesure l'état de sécurité du client.
- *Journaux de validation du client à la page 15-47* donne un aperçu de la manière dont vous pouvez utiliser des journaux pour comprendre l'état de sécurité des clients du réseau.
- *Maintenance des journaux du client à la page 15-47* donne un aperçu de la manière dont vous pouvez assurer la maintenance de la taille des journaux de validation des clients.

- *Tâches administratives à la page 15-47* décrit comment modifier le mot de passe du serveur Policy Server et comment établir un programme de synchronisation.

Configuration du serveur Policy Server depuis OfficeScan

La première étape de la configuration des serveurs Policy Server consiste à ajouter les serveurs Policy Server installés sur le serveur OfficeScan. Vous pouvez ainsi ouvrir la console Web du serveur Policy Server à partir de la console Web d'OfficeScan.

Ajout d'un serveur Policy Server à partir d'OfficeScan

Tâche

1. Dans le menu principal de la console Web d'OfficeScan, cliquez sur **Cisco NAC** > **Serveurs Policy Server**.

   L'écran Serveurs Policy Server apparaît et affiche la liste des serveurs Policy Server.

2. Cliquez sur **Ajouter**.

   L'écran **Serveurs Policy Server** apparaît.

3. Saisissez l'adresse complète du serveur Policy Server et le numéro de port utilisé par le serveur pour les communications HTTPS (par exemple : `https://policy-server:4343/`). Vous pouvez également entrer une description du serveur.

4. Saisissez un mot de passe à utiliser lorsque vous vous connectez à la console Web du serveur Policy Server et confirmez-le.

5. Cliquez sur **Ajouter**.

Suppression d'un serveur Policy Server à partir d'OfficeScan

Tâche

1. Dans le menu principal de la console Web d'OfficeScan, cliquez sur **Cisco NAC** > **Serveurs Policy Server**.

   L'écran **Serveurs Policy Server** apparaît et affiche la liste des serveurs Policy Server.

2. Cochez la case correspondant au serveur Policy Server à supprimer.
3. Cliquez sur **Supprimer**.

Remarque

Pour valider tous les clients du réseau, ajoutez tous les serveurs OfficeScan à au moins un serveur Policy Server.

Résumé des informations d'un serveur Policy Server

L'écran **Résumé** contient des informations à propos du serveur Policy Server, y compris les paramètres de configuration des stratégies et des règles, les journaux de validation des clients et les serveurs OfficeScan enregistrés sur un serveur Policy Server.

L'adresse IP et le numéro de port du serveur de politique pour Cisco NAC apparaissent dans le haut de l'écran **Résumé**.

Le tableau **Résumé de configuration** affiche le nombre de serveurs OfficeScan enregistrés sur le serveur Policy Server, les stratégies du serveur Policy Server et les règles qui composent les stratégies.

Visualisation et modification des détails du résumé de configuration d'un serveur Policy Server :

Tâche

1. Dans le menu principal de la console Web d'OfficeScan, cliquez sur **Cisco NAC** > **Serveurs Policy Server**.

   L'écran **Serveurs Policy Server** apparaît et affiche la liste des serveurs Policy Server.

2. Cliquez sur le nom du serveur Policy Server dont vous souhaitez consulter les informations.

   L'écran **Résumé** apparaît ; il affiche le tableau **Résumé de la configuration**.

3. Cliquez sur le lien en regard de l'élément dont vous souhaitez consulter les paramètres de configuration :

- **Serveur(s) OfficeScan enregistré(s)** : les serveurs OfficeScan actuellement sur le réseau.
- **Stratégies** : stratégies du serveur Policy Server utilisables par les serveurs OfficeScan
- **Règle(s)** : règles du serveur Policy Server composant les stratégies

Conseil

Si vous souhaitez appliquer les mêmes paramètres à plusieurs serveurs Policy Server du réseau, y compris des règles et des stratégies identiques, exportez puis importez les paramètres d'un serveur à un autre. Trend Micro conseille de configurer les mêmes paramètres sur tous les serveurs Policy Server du réseau pour assurer la cohérence de la stratégie antivirus.

Synchronisation du serveur Policy Server avec les serveurs OfficeScan enregistrés

Tâche

1. Dans l'écran **Résumé**, cliquez sur **Synchroniser avec OfficeScan**. L'écran **Résumé - Résultats de la synchronisation** apparaît, contenant les informations suivantes en lecture seule :
   - Nom du serveur **OfficeScan** : le nom de l'hôte ou l'adresse IP et le numéro de port des serveurs OfficeScan enregistrés.
   - **Résultat de la synchronisation** : indique si la synchronisation a réussi.
   - **Dernière synchronisation°**: date de la dernière synchronisation réussie.

Pour plus d'informations sur la synchronisation, voir *Synchronisation à la page 15-18*.

Enregistrement du serveur Policy Server

Enregistrez le serveur Policy Server au moins sur un serveur OfficeScan pour que le serveur Policy Server puisse recevoir les fichiers de signatures de virus et les informations relatives à la version du moteur de scan antivirus. Voir *Séquence de validation*

du client à la page 15-8 pour obtenir des informations sur le rôle que le serveur OfficeScan joue dans le processus de validation.

Remarque

pour que le serveur Policy Server valide tous les clients du réseau, ajoutez tous les serveurs OfficeScan à au moins un serveur Policy Server.

Ajoutez un nouveau serveur OfficeScan ou modifiez les paramètres d'un serveur existant à partir de l'écran Serveurs OfficeScan que vous pouvez afficher en accédant à la console Web du serveur Policy Server, puis en cliquant sur **Configurations** > **Serveurs OfficeScan**.

règles

Les règles sont les unités qui permettent de constituer les stratégies. La configuration des règles constitue l'étape suivante de la configuration du serveur Policy Server. Voir la *Création des règles à la page 15-12* pour plus d'informations.

Pour accéder aux écrans de la console Web pour les règles Cisco ACS, accédez à la console Web Serveur Policy Server et cliquez sur **Configuration** > **Règles** dans le menu principal.

Stratégies

Lorsque vous avez configuré les nouvelles règles ou vérifié que les règles par défaut conviennent à vos besoins de sécurité, configurez des stratégies que les serveurs OfficeScan enregistrés peuvent utiliser. Voir la *Création des stratégies à la page 15-16* pour plus d'informations.

Ajoutez une nouvelle stratégie Cisco NAC ou modifiez une stratégie existante pour déterminer les règles actuellement appliquées et pour agir sur les clients au cas où l'état de sécurité du client ne corresponde à aucune règle.

Pour accéder aux écrans de la console Web pour les stratégies Cisco ACS, accédez à la console Web Serveur Policy Server et cliquez sur **Configuration** > **Stratégies** dans le menu principal.

Journaux de validation du client

Utilisez les journaux de validation des clients pour afficher des informations détaillées sur les clients après validation par le serveur Policy Server. La validation se produit lorsque le serveur ACS récupère les données d'état de sécurité du client et les envoie au serveur Policy Server, qui les compare aux stratégies et aux règles (voir *Séquence de validation du client à la page 15-8*).

Remarque

Pour générer des journaux de validation des clients lors de l'ajout ou de la modification d'une nouvelle règle ou stratégie, cochez la case sous Actions côté serveur.

Pour accéder aux écrans de la console Web pour les journaux Cisco ACS, accédez à la console Web Serveur Policy Server et cliquez sur **Journaux** > **Affichage des journaux de validation du client** dans le menu principal.

Maintenance des journaux du client

Le serveur Policy Server archive les journaux de validation des clients lorsqu'ils atteignent la taille que vous avez indiquée. Il peut également supprimer les fichiers journaux lorsqu'un nombre déterminé de fichiers journaux est atteint. Précisez la manière dont le serveur Policy Server assure la maintenance des journaux de validation des clients en cliquant sur **Journaux** > **Maintenance des journaux** dans la console Web du serveur Policy Server.

Tâches administratives

Exécutez les tâches administratives suivantes sur le serveur Policy Server :

- **Modifier le mot de passe** : modifie le mot de passe configuré lors de l'ajout du serveur Policy Server (voir *Configuration du serveur Policy Server depuis OfficeScan à la page 15-43*)
- **Configurer un programme de synchronisation**°: le serveur Policy Server doit se procurer périodiquement la version du fichier de signatures de virus et du moteur de scan antivirus sur le serveur OfficeScan, afin d'évaluer l'état de sécurité du client OfficeScan. C'est pourquoi vous ne pouvez pas activer ou désactiver la synchronisation programmée. Par défaut, le serveur Policy Server se synchronise

au(x) serveur(s) OfficeScan toutes les cinq minutes (voir *Synchronisation à la page 15-18* pour obtenir des informations complémentaires).

Remarque

Synchronisez manuellement le serveur Policy Server avec le serveur OfficeScan à tout moment dans l'écran Résumé (voir *Résumé des informations d'un serveur Policy Server à la page 15-44*).

Pour accéder aux écrans de la console Web pour les tâches administratives Cisco ACS, accédez à la console Web du serveur Policy Server, puis cliquez sur Administration dans le menu principal.

Chapitre 16

Configuration d'OfficeScan avec des logiciels tiers

Ce chapitre décrit l'intégration d'OfficeScan aux logiciels tiers.

Sujets abordés dans ce chapitre:

- *Aperçu général de l'architecture et de la configuration de Check Point à la page 16-2*
- *Configuration du fichier Secure Configuration Verification pour OfficeScan à la page 16-4*
- *Installation du support SecureClient à la page 16-6*

Aperçu général de l'architecture et de la configuration de Check Point

Intégrez les installations d'OfficeScan à Check Point™ SecureClient™ à l'aide de Secure Configuration Verification (SCV) dans le cadre de l'Open Platform for Security (OPSEC). Reportez-vous à la documentation Check Point SecureClient OPSEC avant de lire cette section. Vous trouverez la documentation d'OPSEC à l'adresse :

http://www.opsec.com

Check Point SecureClient a la possibilité de vérifier la configuration de sécurité des ordinateurs connectés au réseau à l'aide des contrôles Secure Configuration Verification (SCV). Les contrôles SCV sont un ensemble de conditions définissant un système client configuré en toute sécurité. Le logiciel tiers peut communiquer la valeur de ces conditions à Check Point SecureClient. Check Point SecureClient compare alors ces conditions aux conditions du fichier SCV afin de déterminer si le client est considéré comme sécurisé.

Les contrôles SCV sont exécutés régulièrement afin de s'assurer que seuls des systèmes configurés de manière sécurisée sont autorisés à se connecter au réseau.

SecureClient utilise des serveurs Policy Server pour propager des contrôles SCV vers tous les clients enregistrés sur le système. L'administrateur configure les contrôles SCV sur les serveurs Policy Server à l'aide de l'éditeur SCV.

L'éditeur SCV est un outil fourni par Check Point qui vous permet de modifier les fichiers SCV pour la propagation de l'installation du client. Pour faire fonctionner l'éditeur SCV, situez et exécutez le fichier `SCVeditor.exe` sur le serveur Policy Server. Dans l'éditeur SCV, ouvrez le fichier `local.scv` dans le dossier `C:\FW1\NG\Conf` (remplacez `C:\FW1` par le chemin d'installation pour le pare-feu Check Point s'il est différent du chemin par défaut).

Pour obtenir des instructions spécifiques sur l'ouverture et la modification d'un fichier `SCV` à l'aide de l'éditeur SCV, voir *Intégration d'OfficeScan à la page 16-3*.

Intégration d'OfficeScan

Le client OfficeScan transmet régulièrement le numéro de fichier de signatures de virus et le numéro du Moteur de scan antivirus à SecureClient pour vérification. SecureClient compare alors ces valeurs avec les valeurs du fichier client `local.scv`.

Le fichier `local.scv` se présente comme suit si vous l'ouvrez dans un éditeur de texte :

```
(SCVObject

:SCVNames (

: (OfceSCV

:type (plugin)

:parameters (

:CheckType (OfceVersionCheck)

:LatestPatternVersion (701)

:LatestEngineVersion (7.1)

:PatternCompareOp (« >= »)

:EngineCompareOp (« >= »)

)

)

)

:SCVPolicy (

: (OfceSCV)

)

:SCVGlobalParams (

:block_connections_on_unverified (true)

:scv_policy_timeout_hours (24)
```

)

)

Dans cet exemple, le contrôle `SCV` permet de réaliser des connexions par le biais du pare-feu si la version du fichier de signatures est la version 701 ou supérieure et si le numéro du moteur de scan est 7.1 ou ultérieur. Si le moteur de scan ou le fichier de signatures est antérieur, toutes les connexions qui passent par le pare-feu Check Point sont bloquées. Modifiez ces valeurs à l'aide de l'éditeur SCV dans le fichier `local.scv` sur le serveur Policy Server.

Remarque

Check Point ne met pas automatiquement à jour le fichier de signatures et le numéro de version du moteur de scan dans le fichier `SCV`. Lorsqu'OfficeScan met à jour le moteur de scan ou le fichier de signatures, vous devez modifier manuellement la valeur des conditions dans le fichier `local.scv` pour les maintenir à jour. Si vous ne mettez pas à jour les versions du moteur de scan et des signatures, Check Point autorise le trafic qui provient des clients disposant de fichiers de signatures ou de moteurs de scan antérieurs, permettant ainsi un risque potentiel d'infiltration de nouveaux virus dans le système.

Configuration du fichier Secure Configuration Verification pour OfficeScan

Pour modifier le fichier `local.scv`, vous devez télécharger et exécuter l'éditeur SCV (`SCVeditor.exe`).

Tâche

1. Téléchargez `SCVeditor.exe` depuis le site de téléchargement de Check Point.

   L'éditeur SCV fait partie du pack OPSEC SDK.

2. Exécutez `SCVeditor.exe` sur le serveur Policy Server.

   La console de l'éditeur SCV s'affiche à l'écran.

3. Ouvrez le dossier `Produits` et sélectionnez `user_policy_scv`.

4. Cliquez sur **Modifier** > **Produit** > **Modifier**, puis saisissez `OfceSCV` dans le champ **Modifier**. Cliquez sur **OK**.

Remarque

Si le fichier `local.scv` contient déjà des stratégies produit pour un logiciel tiers, créez une nouvelle stratégie en cliquant sur **Modifier** > **Produit** > **Ajouter**, puis saisissez `OfceSCV` dans le champ **Ajouter**.

5. Ajoutez un paramètre en cliquant sur **Modifier** > **Paramètres** > **Ajouter**, puis en saisissant un **Nom** et une **Valeur** dans les champs correspondants.

   Le tableau suivant donne la liste des noms et des valeurs des paramètres. Les noms et les valeurs des paramètres sont sensibles à la casse. Saisissez-les dans l'ordre indiqué dans le tableau.

TABLEAU 16-1. Noms et valeurs des paramètres du fichier SCV

NOM	VALEUR
CheckType	OfceVersionCheck
LatestPatternVersion	<numéro du fichier de signatures actuel>
LatestEngineVersion	<numéro du moteur de scan actuel>
LatestPatternDate	<date d'émission du fichier de signatures actuel>
PatternCompareOp	>=
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	

Saisissez le numéro du fichier de signatures actuel et le numéro du moteur de scan au lieu du texte dans les accolades. Consultez les dernières versions du fichier de signatures de virus et de moteur de scan des clients en cliquant sur **Mise à jour & mise à niveau** dans le menu principal de la console Web d'OfficeScan. Le numéro de la version du fichier de signatures apparaît à droite du graphique circulaire représentant le pourcentage des clients OfficeScan protégés.

6. Sélectionnez **Bloquer les connections avec SCV non vérifié**.
7. Cliquez sur **Modifier** > **Produit** > **Appliquer**.
8. Cliquez sur **Fichier** > **Générer un fichier de stratégie** pour créer le fichier. Sélectionnez le fichier existant `local.scv` pour l'écraser.

Installation du support SecureClient

Si des utilisateurs se connectent au réseau de l'entreprise via un réseau privé virtuel (RPV) et qu'ils disposent à la fois de Check Point SecureClient et du client OfficeScan sur leur ordinateur, demandez-leur d'installer le support SecureClient. Ce module permet à SecureClient d'exécuter régulièrement des contrôles SCV sur les clients RPV afin de s'assurer que seuls des systèmes configurés soient autorisés à se connecter au réseau. Les utilisateurs peuvent vérifier que Check Point SecureClient est installé sur leur ordinateur en vérifiant la présence de l'icône ( ) dans la barre d'état système. Les utilisateurs peuvent également vérifier si un élément nommé **Check Point SecureClient** est présent dans l'écran **Ajout/Suppression de programmes** de Windows.

Les utilisateurs lancent l'installation à partir de l'onglet **Boîte à outils** de la console du client OfficeScan. Cet onglet ne s'affiche que si les utilisateurs ont les droits nécessaires

et si le système d'exploitation des ordinateurs du client OfficeScan est Windows XP ou Windows Server 2003.

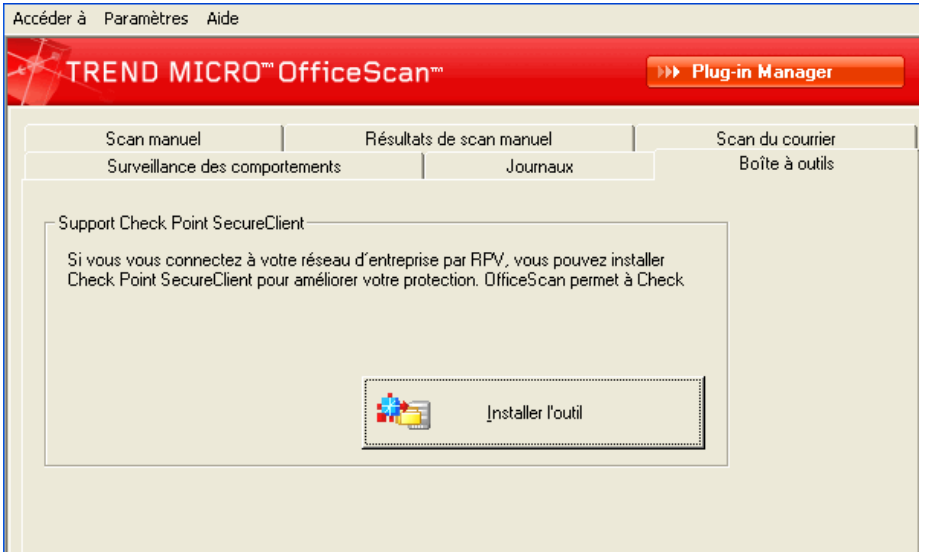


FIGURE 16-1. Onglet Boîte à outils sur la console du client OfficeScan

Accord de privilège d'affichage de l'onglet Boîte à outils pour les utilisateurs

Tâche

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence des clients, cliquez sur l'icône du domaine racine. ( ) pour inclure tous les clients ou spécifier les domaines ou clients.

Remarque

Le programme de support Check Point SecureClient ne prend pas en charge IPv6. Vous ne pouvez pas déployer ce module aux points finaux IPv6 purs.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges de la boîte à outils**.

5. Sélectionnez **Afficher l'onglet Boîte à outils sur la console client et autoriser les utilisateurs à installer le support Check Point SecureClient**.

6. Si vous avez sélectionné un ou plusieurs domaines ou clients dans l'arborescence client, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône du domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les clients** : applique les paramètres à tous les clients existants et à tout nouveau client ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux clients ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux clients ajoutés à un domaine existant.

Installation du support SecureClient

Tâche

1. Ouvrez la console du client OfficeScan.

2. Cliquez sur l'onglet **Boîte à outils**.

3. Dans **Support Check Point SecureClient**, cliquez sur **Installer/Mettre à niveau le support SecureClient**.

   Un écran de confirmation s'affiche.

4. Cliquez sur **Oui**.

   Le client OfficeScan se connecte au serveur et télécharge le module. OfficeScan affiche un message lorsque le téléchargement est terminé.

5. Cliquez sur **OK**.

Chapitre 17

Obtenir de l'aide

Ce chapitre explique les problèmes de dépannage pouvant survenir et indique comment contacter le support.

Sujets abordés dans ce chapitre:

- *Ressources de dépannage à la page 17-2*
- *Comment contacter l?assistance technique à la page 17-24*

Ressources de dépannage

Cette section met à votre disposition une liste de ressources qui permettent de résoudre les problèmes liés au serveur OfficeScan et au client OfficeScan.

- *Support Intelligence System à la page 17-2*
- *Case Diagnostic Tool à la page 17-2*
- *Journaux du serveur OfficeScan à la page 17-3*
- *Journaux du client OfficeScan à la page 17-15*

Support Intelligence System

Support Intelligence System est une page depuis laquelle vous pouvez facilement envoyer des fichiers à Trend Micro à des fins d'analyse. Ce système détecte le GUID du serveur OfficeScan et joint cette information au fichier que vous envoyez. En joignant ce GUID, vous permettez à Trend Micro de vous fournir un retour d'informations sur les fichiers envoyés pour évaluation.

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collecte les informations de débogage nécessaires issues du produit d'un client à chaque fois qu'un problème apparaît. Il active ou désactive automatiquement le débogage du produit et collecte les fichiers nécessaires en fonction des catégories de problèmes. Trend Micro utilise ces informations pour résoudre les problèmes liés au produit.

Exécutez l'outil sur toutes les plates-formes prises en charge par OfficeScan. Pour obtenir cet outil et la documentation appropriée, contactez votre service d'assistance.

Trend Micro Performance Tuning Tool

Trend Micro fournit un outil autonome d'optimisation des performances pour identifier les applications susceptibles de provoquer des problèmes de performances. Trend Micro Performance Tuning Tool, disponible dans la base de connaissances de Trend Micro,

doit être exécuté sur une image de poste de travail autonome et/ou sur quelques postes de travail cibles durant le processus pilote pour éviter les problèmes de performances dans le déploiement réel de la surveillance des comportements et du contrôle des dispositifs.

Remarque

Trend Micro Performance Tuning Tool ne prend en charge que les plates-formes 32 bits.

Pour plus d'informations, consultez *Base de connaissances* de Trend Micro.

Journaux du serveur OfficeScan

En plus des journaux disponibles sur la console Web, vous pouvez utiliser d'autres types de journaux (tels que les journaux de débogage) pour résoudre les problèmes liés aux produits.

AVERTISSEMENT!

Les journaux de débogage risquent de diminuer les performances du serveur et utilisent une quantité considérable d'espace disque. Activez la journalisation du débogage si nécessaire et désactivez-la immédiatement si vous n'utilisez plus les données de débogage. Supprimez le fichier journal si vous avez besoin d'espace disque.

Journaux de débogage du serveur à l'aide de LogServer.exe

Utilisez `LogServer.exe` afin de collecter les journaux de débogage pour les entités suivantes :

- Journaux de base du serveur OfficeScan
- Trend Micro Vulnerability Scanner
- Journaux d'intégration d'Active Directory
- Journaux de regroupement des clients
- Journaux de conformité de la sécurité
- Administration basée sur les rôles

- Smart scan
- Policy Server

Activation de la journalisation du débogage

Tâche

1. Connectez-vous à la console Web.
2. Dans la bannière de la console Web, cliquez sur le premier « O » dans « OfficeScan ».
3. Spécifiez les paramètres de journalisation du débogage.
4. Cliquez sur **Enregistrer**.
5. Vérifiez le fichier journal (`ofcdebug.log`) dans son emplacement par défaut : <*Dossier d'installation du serveur*>`\PCCSRV\Log`.

Désactivation de la journalisation du débogage

Tâche

1. Connectez-vous à la console Web.
2. Dans la bannière de la console Web, cliquez sur le premier « O » dans « OfficeScan ».
3. Désactivez **Activer le journal de débogage**.
4. Cliquez sur **Enregistrer**.

Activation de la journalisation du débogage pour l'installation et la mise à niveau du serveur

Activez la journalisation du débogage avant d'exécuter les tâches suivantes:

- Désinstaller et réinstaller le serveur.
- Procéder à une mise à niveau d'OfficeScan vers une nouvelle version.

- Exécuter une installation/mise à niveau à distance (la journalisation du débogage est activée sur l'ordinateur sur lequel vous avez lancé l'installation et non sur l'ordinateur distant).

Tâche

1. Copiez le dossier `LogServer` situé dans <*Dossier d'installation du serveur*>`\PCCSRV\Private` dans `C:\`.
2. Créez un fichier nommé `cdebug.ini` avec le contenu suivant :

   ```
   [debug]

   debuglevel=9

   debuglog=c:\LogServer\ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

3. Enregistrez `ofcdebug.ini` dans `C:\LogServer`.
4. Exécutez la tâche appropriée (c'est-à-dire, désinstaller/réinstaller le serveur, mettre à niveau vers une nouvelle version ou exécuter une installation/mise à niveau à distance).
5. Vérifiez le fichier ofcdebug.log dans `C:\LogServer`.

Journaux d'installation

- Journaux d'installation/de mise à niveau locale

  Nom du fichier : `OFCMAS.LOG`

  Emplacement : `%windir%`

- Journaux d'installation/de mise à niveau à distance
  - Sur l'ordinateur sur lequel vous avez lancé l'installation:

Nom du fichier : `ofcmasr.log`

Emplacement : `%windir%`

- Sur l'ordinateur cible:

  Nom du fichier : `OFCMAS.LOG`

  Emplacement : `%windir%`

Journaux Active Directory

- **Nom du fichier** : `ofcdebug.log`
- **Nom du fichier** : `ofcserver.ini`

  Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Private\`
- **Noms de fichiers** :
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  Emplacement : `<Dossier d'installation du serveur>\PCCSRV\HTTPDB\`

Journaux de Role-based Administration

Pour des informations détaillées sur l'administration basée sur les rôles, effectuez l'une des opérations suivantes:

- Lancez Trend Micro Case Diagnostics Tool. Pour plus d'informations, consultez *Case Diagnostic Tool à la page 17-2*.
- Rassemblez les journaux suivants:

- Tous les fichiers situés dans <*Dossier d'installation du serveur*>\PCCSRV\Private\AuthorStore.
- *Journaux du serveur OfficeScan à la page 17-3*

Journaux de regroupement du client OfficeScan

- **Nom du fichier** : ofcdebug.log
- **Nom du fichier** : ofcserver.ini

  Emplacement : <*Dossier d'installation du serveur*>\PCCSRV\Private\
- **Nom du fichier** : SortingRule.xml

  Emplacement : <Dossier d'installation du serveur>\PCCSRV\Private\SortingRuleStore\
- **Noms de fichiers** :
  - dbADScope.cdx
  - dbADScope.dbf

  Emplacement : <Dossier d'installation du serveur>\HTTPDB\

Journaux de mise à jour des composants

Nom du fichier : TmuDump.txt

Emplacement : <*Dossier d'installation du serveur*>\PCCSRV\Web\Service\AU_Data\AU_Log

Obtention d'informations détaillées sur la mise à jour du serveur

Tâche

1. Créez un fichier nommé aucfg.ini avec le contenu suivant :

   ```
   [Debug]

   level=-1
   ```

```
[Downloader]

ProxyCache=0
```

2. Enregistrez le fichier dans <*Dossier d'installation du serveur*>\PCCSRV\Web\Service.

3. Redémarrez le service principal d'OfficeScan.

Arrêt de la collecte d'informations détaillées sur la mise à jour du serveur

---

Tâche

1. Supprimez le fichier `aucfg.ini`.

2. Redémarrez le service principal d'OfficeScan.

Journaux du serveur Apache

Noms de fichiers :

- `install.log`
- `error.log`
- `access.log`

Emplacement : <*Dossier d'installation du serveur*>\PCCSRV\Apache2

Journaux de Client Packager

Activation de la journalisation pour la création de Client Packager

---

Tâche

1. Modifiez le fichier `ClnExtor.ini`situé dans <*Dossier d'installation du serveur*>\PCCSRV\Admin\Utility\ClientPackagercomme suit :

```
[Common]
```

```
DebugMode=1
```

2. Vérifiez le fichier `ClnPack.log` dans `C:\`.

Désactivation de la journalisation pour la création de Client Packager

Tâche

1. Ouvrez le fichier `ClnExtor.ini`.
2. Remplacez la valeur 3 de «DebugMode» par 0.

Journaux de rapport de conformité de la sécurité

Pour obtenir des informations détaillées sur la conformité de la sécurité, rassemblez les informations suivantes :

- **Nom du fichier** : `RBAUserProfile.ini`

  Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Private\AuthorStore\`

- Tous les fichiers dans `<Dossier d'installation du serveur>\PCCSRV\Log\Security Compliance Report`.
- *Journaux du serveur OfficeScan à la page 17-3*

Journaux de gestion des serveurs externes

- **Nom du fichier** : `ofcdebug.log`
- **Nom du fichier** : `ofcserver.ini`

  Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Private\`

- Tous les fichiers situés dans `<Dossier d'installation du serveur>\PCCSRV\Log\Outside Server Management Report\`.
- **Noms de fichiers** :
  - `dbADScope.cdx`

- `dbADScope.dbf`
- `dbClientInfo.cdx`
- `dbclientInfo.dbf`

Emplacement : `<Dossier d'installation du serveur>\HTTPDB\`

Journaux d'exceptions du contrôle des dispositifs

Pour obtenir des informations détaillées sur les exceptions du contrôle des dispositifs, rassemblez les informations suivantes :

- **Nom du fichier** : `ofcscan.ini`

  Emplacement : <*Dossier d'installation du serveur*>\
- **Nom du fichier** : `dbClientExtra.dbf`

  Emplacement : `<Dossier d'installation du serveur>\HTTPDB\`
- Liste d'exceptions du contrôle des dispositifs sur la console Web d'OfficeScan.

Journaux de réputation de sites Web

Nom du fichier : `diagnostic.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\LWCS\`

Journaux de l'outil ServerProtect Normal Server Migration

Activation de la journalisation du débogage pour l'outil ServerProtect Normal Server Migration

Tâche

1. Créez un fichier nommé `ofcdebug.ini` avec le contenu suivant :

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. Enregistrez le fichier sous `C:\`.
3. Vérifiez le fichier `ofcdebug.log` dans `C:\`.

Remarque

Pour désactiver la journalisation du débogage, supprimez le fichier `ofcdebug.ini`.

Journaux de VSEncrypt

OfficeScan crée automatiquement ce journal de débogage (`VSEncrypt.log`) dans le dossier temporaire du compte utilisateur. Par exemple, dans `C:\Documents and Settings\<Nom de l'utilisateur>\Local Settings\Temp`.

Journaux de l'agent MCP de Control Manager

Fichiers de débogage situés dans <*Dossier d'installation du serveur*>`\PCCSRV\CMAgent`

- `Agent.ini`
- `Product.ini`
- Capture d'écran de la page des paramètres de Control Manager
- `ProductUI.zip`

Activation de la journalisation du débogage pour l'agent MCP

Tâche

1. Modifiez le fichier `product.ini` situé dans <*Dossier d'installation du serveur*>`\PCCSRV\CmAgent` comme suit :

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000
```

```
debuglog = C:\CMAgent_debug.log
```

2. Redémarrez le service Control Manager Agent d'OfficeScan depuis Microsoft Management Console.
3. Vérifiez le fichier `CMAgent_debug.log` dans `C:\`.

Désactivation de la journalisation du débogage pour l'agent MCP

Tâche

1. Ouvrez le fichier `product.ini` et supprimez les éléments suivants :

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Redémarrez le service OfficeScan Control Manager.

Journaux du moteur de scan antivirus

Activation de la journalisation du débogage pour le Moteur de scan antivirus

---

Tâche

1. Ouvrez l'éditeur de la base de registre (`regedit.exe`).
2. Accédez à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.
3. Remplacez la valeur de la variable « `DebugLogFlags` » par « `00003eff` ».
4. Exécutez les étapes ayant mené au problème de scan que vous avez rencontré.

5. Vérifiez le fichier `TMFilter.log` dans `%windir%`.

Remarque

Désactivez la journalisation du débogage en réaffectant à la variable « `DebugLogFlags` » la valeur « `00000000` »

Journaux de virus/programmes malveillants

Nom du fichier :

- `dbVirusLog.dbf`
- `dbVirusLog.cdx`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\HTTPDB\`

Journaux de spywares/graywares

Nom du fichier :

- `dbSpywareLog.dbf`
- `dbSpywareLog.cdx`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\HTTPDB\`

Journaux des épidémies

Journaux actuels des épidémies de violation de pare-feu

Nom du fichier : `Cfw_Outbreak_Current.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Log\`

Derniers journaux des épidémies de violation de pare-feu

Nom du fichier : `Cfw_Outbreak_Last.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Log\`

Journaux actuels des épidémies de virus/programmes malveillants

Nom du fichier : `Outbreak_Current.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Log\`

Derniers journaux des épidémies de virus/programmes malveillants

Nom du fichier : `Outbreak_Last.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Log\`

Journaux actuels des épidémies de spywares/graywares

Nom du fichier : `Spyware_Outbreak_Current.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Log\`

Derniers journaux des épidémies de spywares/graywares

Nom du fichier : `Spyware_Outbreak_Last.log`

Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\Log\`

Journaux de Virtual Desktop Support

- **Nom du fichier** : `vdi_list.ini`

  Emplacement : <*Dossier d'installation du serveur*>`\PCCSRV\TEMP\`

- **Nom du fichier** : `vdi.ini`

  Emplacement : `<Dossier d'installation du serveur>\PCCSRV\Private\`

- **Nom du fichier** : `ofcdebug.txt`

  Emplacement : `<Dossier d'installation du serveur>\PCCSRV\`

Pour générer `ofcdebug.txt`, activez la journalisation du débogage. Pour plus d'informations sur l'activation de la journalisation du débogage, voir *Activation de la journalisation du débogage à la page 17-4*.

Journaux du client OfficeScan

Utilisez les journaux du client OfficeScan (comme les journaux de débogage) pour résoudre les problèmes liés au client OfficeScan.

AVERTISSEMENT!

Les journaux de débogage risquent de diminuer les performances du client et utilisent une quantité considérable d'espace disque. Activez la journalisation du débogage si nécessaire et désactivez-la immédiatement si vous n'utilisez plus les données de débogage. Supprimez le fichier journal si la taille du fichier devient trop volumineuse.

Journaux de débogage du client OfficeScan à l'aide de LogServer.exe

Activation de la journalisation du débogage pour le client OfficeScan

Tâche

1. Créez un fichier nommé `ofcdebug.ini` avec le contenu suivant :

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. Envoyez le fichier `ofcdebug.ini` aux utilisateurs clients en leur demandant de l'enregistrer sous `C:\`.

Remarque

Le fichier `LogServer.exe` s'exécute automatiquement à chaque redémarrage de l'ordinateur client OfficeScan. Demandez aux utilisateurs de ne PAS fermer la fenêtre de commande LogServer.exe qui s'ouvre au démarrage de l'ordinateur car cette opération invite OfficeScan à interrompre la journalisation de débogage. Si les utilisateurs ferment la fenêtre de commande, ils peuvent relancer la journalisation du débogage en exécutant le fichier `LogServer.exe` situé dans <*Dossier d'installation du client*>.

3. Pour chaque ordinateur du client OfficeScan, vérifiez le fichier ofcdebug.log dans C:\.

Remarque

Désactivez la journalisation du débogage pour le client OfficeScan en supprimant le fichier `ofcdebug.ini`.

Journaux des nouvelles installations

Nom du fichier : `OFCNT.LOG`

Emplacements :

- `%windir%` pour toutes les méthodes d'installation à l'exception du pack MSI
- `%temp%` pour la méthode d'installation à l'aide du pack MSI

Journaux des mises à niveau/correctifs de type hotfix

Nom du fichier : `upgrade_yyyymmddhhmmss.log`

Emplacement : <*Dossier d'installation du client*>

Journaux de Damage Cleanup Services

Activation de la journalisation du débogage pour Damage Cleanup Services

Tâche

1. Ouvrez le fichier `TSC.ini` situé dans <*Dossier d'installation du client*>.
2. Modifiez la ligne suivante comme suit:

   ```
   DebugInfoLevel=3
   ```

3. Vérifiez le fichier `TSCDebug.log` situé dans `<Dossier d'installation du client>\debug`.

Activation de la journalisation du débogage pour Damage Cleanup Services

Ouvrez le fichier `TSC.ini` et remplacez la valeur 3 de la variable « `DebugInfoLevel` » par 0.

Journal Cleanup

Nom du fichier : `yyyymmdd.log`

Emplacement : <*Dossier d'installation du client*>`\report\`

Journaux de scan de courrier

Nom du fichier : `SmolDbg.txt`

Emplacement : <*Dossier d'installation du client*>

Journaux ActiveUpdate

- **Nom du fichier** : `Update.ini`

  Emplacement : <*Dossier d'installation du client*>

- **Nom du fichier** : `TmuDump.txt`

Emplacement : `<Dossier d'installation du client>\AU_Log\`

Journaux de connexion du client OfficeScan

Nom du fichier : `Conn_YYYYMMDD.log`

Emplacement : <*Dossier d'installation du client*>`\ConnLog`

Journaux de mise à jour du client OfficeScan

Nom du fichier : `Tmudump.txt`

Emplacement : <*Dossier d'installation du client*>`\AU_Data\AU_Log`

Obtention d'informations sur la mise à jour du client OfficeScan

Tâche

1. Créez un fichier nommé `aucfg.ini` avec le contenu suivant :

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. Enregistrez le fichier dans <*Dossier d'installation du client*>.

3. Rechargez le client OfficeScan.

Remarque

Cessez de collecter les informations détaillées sur les mises à jour en supprimant le fichier `aucfg.ini` et en rechargeant le client OfficeScan.

Journaux de prévention des épidémies

Nom du fichier : `OPPLogs.log`

Emplacement : <*Dossier d'installation du client*>\OppLog

Journaux de rétablissement de la prévention des épidémies

Noms de fichiers :

- TmOPP.ini
- TmOPPRestore.ini

Emplacement : <*Dossier d'installation du client*>\

Journaux du pare-feu OfficeScan

Activation de la journalisation du débogage pour le pilote de pare-feu commun sur les ordinateurs Windows Vista/Server 2008/7

Tâche

1. Modifiez les valeurs de registre suivantes :

CLÉ DE REGISTRE	VALEURS
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	**Type** : Valeur DWORD (REG_DWORD) **Nom**: DebugCtrl **Valeur** : 0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	**Type** : Valeur DWORD (REG_DWORD) **Nom**: DebugCtrl **Valeur** : 0x00001111

2. Redémarrez l'ordinateur.
3. Vérifiez les fichiers wfp_log.txt et lwf_log.txt dans C:\.

Activation de la journalisation du débogage pour le pilote de pare-feu commun sur les ordinateurs Windows XP et Windows Server 2003

Tâche

1. Ajoutez les données suivantes dans `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters` :
   - **Type** : Valeur `DWORD (REG_DWORD)`
   - **Nom**: `DebugCtrl`
   - **Valeur** : `0x00001111`
2. Redémarrez l'ordinateur.
3. Vérifiez le fichier `cfw_log.txt` dans `C:\`.

Désactivation de la journalisation du débogage pour Pilote du pare-feu commun (tous les systèmes d'exploitation)

Tâche

1. Supprimez « `DebugCtrl` » dans la clé de registre.
2. Redémarrez l'ordinateur.

Activation de la journalisation du débogage pour le service de pare-feu OfficeScan NT

Tâche

1. Modifiez le fichier `TmPfw.ini` situé dans <*Dossier d'installation du client*> comme suit :

   ```
   [ServiceSession]

   Enable=1
   ```

2. Rechargez le client.

3. Vérifiez `ddmmyyyy_NSC_TmPfw.log` dans `C:\temp`.

Désactivation de la journalisation du débogage pour le service de pare-feu OfficeScan NT

Tâche

1. Ouvrez le fichier `TmPfw.ini` et remplacez la valeur 1 de la variable « `Enable` » par 0.
2. Rechargez le client OfficeScan.

Journaux de la réputation de sites Web et du scan de la messagerie POP3

Activation de la journalisation du débogage pour les fonctions de réputation de sites Web et de scan de la messagerie POP3

Tâche

1. Modifiez le fichier `TmProxy.ini`situé dans <*Dossier d'installation du client*> comme suit :

```
[ServiceSession]

Enable=1

LogFolder=C:\temp
```

2. Rechargez le client OfficeScan.
3. Vérifiez `ddmmyyyy_NSC_TmProxy.log` dans `C:\temp`.

Désactivation de la journalisation du débogage pour les fonctions de réputation de sites Web et de scan de la messagerie POP3

Tâche

1. Ouvrez le fichier `TmProxy.ini` et remplacez la valeur 1 de la variable « `Enable` » par 0.
2. Rechargez le client OfficeScan.

Journaux de listes d'exceptions du contrôle des dispositifs

Nom du fichier : `DAC_ELIST`

Emplacement : <*Dossier d'installation du client*>\

Journaux de débogage de protection des données

Activation de la journalisation de débogage pour le module Protection des données

Tâche

1. Obtenez le fichier `logger.cfg` auprès de votre service d'assistance.
2. Ajoutez les données suivantes dans `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
   - **Type** : `chaîne`
   - **Nom**: `debugcfg`
   - **Valeur** : `C:\Log\logger.cfg`
3. Créez un dossier intitulé « Log » dans le `C:\ directory`.
4. Copiez le fichier `logger.cfg` dans le dossier « Log ».
5. Déployez la prévention contre la perte des données et les paramètres de contrôle des dispositifs depuis la console Web pour lancer la collecte de journaux.

Remarque

Désactivez la journalisation de débogage pour le module Protection des données en supprimant `debugcfg` dans la clé de registre et en redémarrant l'ordinateur.

Journaux des événements Windows

L'Observateur d'événements de Windows affiche les événements d'application, tels que les connexions ou les modifications de paramètres de compte.

Tâche

1. Effectuez l'une des actions suivantes:
   - Cliquez sur **Démarrer** > **Panneau de configuration** > **Performances et maintenance** > **Outils administrateurs** > **Gestion de l'ordinateur**.
   - Ouvrez MMC, qui contient le composant logiciel enfichable Observateur d'événements.
2. Cliquez sur **Observateur d'événements**.

Journaux de l'interface Transport Driver Interface (TDI)

Activation de la journalisation du débogage pour TDI

Tâche

1. Ajoutez les données suivantes dans `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters` :

PARAMÈTRE	VALEURS
Clé 1	**Type** : Valeur `DWORD (REG_DWORD)` **Nom**: `Déboguer` **Valeur** : `1111 (hexadécimal)`

PARAMÈTRE	VALEURS
Clé 2	**Type** : `valeur de chaîne (REG_SZ)` **Nom**: `LogFile` **Valeur** : `C:\tmtdi.log`

2. Redémarrez l'ordinateur.
3. Vérifiez le fichier `tmtdi.log` dans `C:\`.

Remarque

Désactivez la journalisation du débogage pour TDI en supprimant les fichiers `Debug` et `LogFile` dans la clé de registre, puis redémarrez l'ordinateur.

Comment contacter l?assistance technique

Trend Micro fournit une assistance technique, des téléchargements de signatures et des mises à jour de programmes à tous les utilisateurs enregistrés pendant une année. Au terme de cette période, un paiement sera exigé pour renouveler la maintenance. Si vous avez besoin d'aide ou si vous avez simplement une question, n'hésitez pas à nous contacter. Vos commentaires sont aussi toujours les bienvenus.

Sites d'assistance à travers le monde :

http://www.trendmicro.com/support

Documentation des produits Trend Micro :

http://docs.trendmicro.com/fr-fr/home.aspx

Contact

Aux États-Unis, vous pouvez contacter les revendeurs Trend Micro par téléphone, fax ou e-mail :

Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014

Numéro gratuit : +1 (800) 228-5651 (ventes) Tél : +1 (408) 257-1500 (ligne principale) Fax : +1 (408) 257-2003

Adresse Web : www.trendmicro.com

E-mail : support@trendmicro.com

Optimisation de votre demande d'assistance

Lorsque vous contactez Trend Micro, rassemblez les informations suivantes pour accélérer la résolution de vos problèmes :

- Versions de Microsoft Windows et du Service Pack
- Type de réseau
- Marque de l'ordinateur, modèle et tout matériel complémentaire connecté à votre ordinateur
- Mémoire et espace disque disponibles sur votre ordinateur
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché
- Étapes permettant de reproduire le problème

Base de connaissances Trend Micro

La base de connaissances Trend Micro, gérée au niveau du site Web de Trend Micro, contient des réponses à jour aux questions sur les produits. Il est possible d'y poser une question si vous ne trouvez pas de réponse dans la documentation du produit. Accédez à la base de connaissances à l'adresse suivante :

http://esupport.trendmicro.com/en-us/enterprise/default.aspx

Trend Micro met à jour en permanence la base de connaissance et ajoute de nouvelles solutions quotidiennement. Cependant, si vous ne trouvez pas de réponse à une question, vous pouvez décrire le problème dans un e-mail et l'envoyer directement à un ingénieur d'assistance Trend Micro qui l'étudiera et le résoudra dès que possible.

TrendLabs

Les TrendLabs ^{SM} constituent le centre d'assistance et de recherche antivirus mondial de Trend Micro. Présent sur trois continents, les TrendLabs emploient plus de 250 chercheurs et ingénieurs qui travaillent jour et nuit pour vous fournir service et assistance ainsi qu'à chaque client de Trend Micro.

Les TrendLabs fournissent les services après-vente suivants :

- Mises à jour régulières des fichiers de signatures pour tous les virus et codes malveillants connus, « en cage » et « en circulation »
- Aide d'urgence en cas d'épidémie virale
- Contact par e-mail avec les ingénieurs antivirus
- Base de connaissances de Trend Micro en ligne, répertoriant les problèmes techniques connus

Les TrendLabs ont obtenu la certification d'assurance qualité ISO 9002.

Centre d'informations de sécurité

Des informations de sécurité complètes sont disponibles sur le site Web de Trend Micro :

- Liste des virus et des codes mobiles malveillants actuellement « en circulation » ou actifs
- Canulars informatiques
- Informations sur les menaces Internet
- Rapport hebdomadaire sur les virus
- Encyclopédie virale contenant une liste complète des noms et des symptômes des virus et codes mobiles malicieux connus
- Glossaire terminologique
- http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp

Envoi de fichiers suspects à Trend Micro

Si vous soupçonnez un fichier d'être infecté et que le moteur de scan ne le détecte pas ou ne peut pas le nettoyer, Trend Micro vous invite à lui envoyer le fichier suspect.

Vous pouvez également envoyer à Trend Micro l'URL de tout site Web que vous pensez être un site de phishing ou un autre « vecteur de menaces » (source de menaces Internet intentionnelles telles que les spywares et les virus).

- Envoyez un e-mail à l'adresse suivante°: virusresponse@trendmicro.com avec le titre «°Phishing ou vecteur de menace°» en objet.
- Utilisez le format d'envoi en ligne à l'adresse suivante°:

  http://subwiz.trendmicro.com/subwiz

Commentaires relatifs à la documentation

Trend Micro cherche toujours à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez consulter le site suivant°:

http://www.trendmicro.com/download/documentation/rating.asp

Annexe A

Prise en charge de l'adressage IPv6 dans OfficeScan

Cette annexe doit être lue par les utilisateurs qui prévoient de déployer OfficeScan dans un environnement prenant en charge l'adressage IPv6. Cette annexe contient des informations sur le degré de prise en charge d'IPv6 dans OfficeScan.

Trend Micro suppose que le lecteur est familiarisé avec les concepts d'IPv6 et les tâches qu'implique la configuration d'un réseau prenant en charge l'adressage IPv6.

Prise en charge de l'adressage IPv6 pour les serveurs et les clients OfficeScan.

Cette version 10.6 est la première à prendre en charge l'adressage IPv6 pour OfficeScan. Les versions précédentes de OfficeScan ne prennent pas en charge l'adressage IPv6. La prise en charge de l'adressage IPv6 est automatiquement activée après l'installation ou la mise à niveau du serveur OfficeScan et des clients OfficeScan remplissant les exigences de l'adressage IPv6.

Configuration requise pour le serveur OfficeScan

Les exigences IPv6 pour le serveur OfficeScan sont les suivantes :

- Le serveur doit être installé sur Windows Server 2008. Il ne peut être installé sur Windows Server 2003, car ce système d'exploitation ne prend que partiellement en charge l'adressage IPv6.
- Le serveur doit utiliser un serveur Web IIS. Le serveur Web Apache ne prend pas en charge l'adressage IPv6.
- Si le serveur peut gérer les clients OfficeScan IPv4 et IPv6, il doit contenir les adresses IPv4 et IPv6 et doit être identifié par son nom d'hôte. Si un serveur est identifié par ses adresses IPv4, les clients OfficeScan IPv6 ne peuvent pas s'y connecter. La même erreur se produit si les clients utilisant exclusivement IPv4 se connectent à un serveur identifié par ses adresses IPv6.
- Si le serveur ne gère que des clients IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6. Lorsque le serveur est identifié par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.

Remarque

Le nom de domaine complet ne peut être spécifié que lors de l'installation locale du serveur. Il n'est pas pris en charge pour les installations à distance.

Configuration requise pour le client OfficeScan

Le client OfficeScan doit être installé sur :

- Windows 7
- Windows Server 2008
- Windows Vista

Il ne peut être installé sur Windows Server 2003 ni Windows XP car ces systèmes d'exploitation ne prennent que partiellement en charge l'adressage IPv6.

Il est préférable qu'un client OfficeScan possède à la fois des adresses IPv4 et IPv6, car certaines entités auxquelles il se connecte ne prennent en charge que l'adressage IPv4.

Limitations des serveurs IPv6 purs

Le tableau suivant répertorie les restrictions pour un serveur OfficeScan possédant uniquement des adresses IPv6.

TABLEAU A-1. Limitations des serveurs IPv6 purs

PHASE	RESTRICTION
Gestion des clients	Un serveur IPv6 ne peut : • Déployer des clients OfficeScan dans des points finaux IPv4 purs. • Gérer des clients OfficeScan IPv4 purs.

PHASE	RESTRICTION
Mises à jour et gestion centralisée	Un serveur IPv6 pur ne peut effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que : • Trend Micro ActiveUpdate Server • Control Manager 5.5 • Control Manager 5.0 **Remarque** L'adressage IPv6 est pris en charge pour Control Manager à partir de la version 5.5 SP1. • Toute source de mise à jour personnalisée IPv4 pure
Enregistrement, activation et renouvellement du produit	Un serveur IPv6 pur ne peut se connecter au serveur d'enregistrement en ligne de Trend Micro pour enregistrer le produit, obtenir la licence et activer/renouveler la licence.
Connexion Proxy	Un serveur IPv6 pur ne peut se connecter via un serveur proxy IPv4 pur.
Solutions de plug-in	Un serveur IPv6 pur possède Plug-In Manager mais ne peut déployer aucune des solutions de plug-in pour : • les clients OfficeScan IPv4 purs ou les hôtes IPv4 purs (du fait de l'absence de connexion directe) ; • les clients OfficeScan IPv6 purs ou les hôtes IPv6 purs, car aucune des solutions de plug-in ne prend en charge IPv6.

La plupart de ces restrictions peuvent être surmontées en configurant un serveur proxy à double pile pouvant convertir les adresses IPv4 et IPv6 (tel que DeleGate). Positionnez le serveur proxy entre le serveur OfficeScan et les entités auxquelles il se connecte ou les entités qu'il dessert.

Limitations des clients OfficeScan IPv6 purs

Le tableau suivant répertorie les restrictions pour un client OfficeScan possédant uniquement une adresse IPv6.

TABLEAU A-2. Limitations des clients OfficeScan IPv6 purs

PHASE	RESTRICTION
Serveur OfficeScan parent	Les clients OfficeScan IPv6 purs ne peuvent être gérés par un serveur OfficeScan IPv4 pur.
Mises à jour	Un client OfficeScan IPv6 ne peut effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que : • Trend Micro ActiveUpdate Server • un serveur OfficeScan IPv4 pur • un agent de mise à jour IPv4 pur • Toute source de mise à jour personnalisée IPv4 pure
Requêtes de scan, requêtes de réputation de sites Web et Smart Feedback	Un client OfficeScan IPv6 pur ne peut envoyer de requêtes à des sources Smart Protection telles que : • Smart Protection Server 2.0 (intégré ou autonome) **Remarque** IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5. • Trend Micro Smart Protection Network (également pour Smart Feedback)
Sécurité des logiciels	Les clients OfficeScan IPv6 purs ne peuvent se connecter au service Certified Safe Software Service hébergé par Trend Micro.
Solutions de plug-in	Les clients OfficeScan IPv6 purs ne peuvent installer de solutions de plug-in car aucune solution ne prend en charge IPv6.
Programmes	Les clients OfficeScan IPv6 purs ne peuvent installer les programmes suivants car ils ne prennent pas en charge IPv6 : • Cisco Trust Agent • Support Check Point SecureClient

PHASE	RESTRICTION
Connexion Proxy	Un client OfficeScan IPv6 pur ne peut se connecter via un serveur proxy IPv4 pur.

La plupart de ces restrictions peuvent être surmontées en configurant un serveur proxy à double pile pouvant convertir les adresses IPv4 et IPv6 (tel que DeleGate). Placez le serveur proxy entre les clients OfficeScan et les entités auxquelles ils se connectent.

Configuration des adresses IPv6

La console Web vous permet de configurer une adresse IPv6 ou une plage d'adresses IPv6. Voici quelques instructions de configuration.

- OfficeScan accepte les présentation d'adresse IPv6 standard.

  Par exemple :

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- OfficeScan accepte également les adresses IPv6 avec un lien local, telles que :

  `fe80::210:5aff:feaa:20a2`

  AVERTISSEMENT!

  Faites attention lors de la spécification d'une adresse IPv6 avec un lien local car, même si OfficeScan accepte cette adresse, il se peut qu'il ne fonctionne pas comme attendu dans certaines circonstances. Par exemple, les clients OfficeScan ne peuvent pas effectuer de mise à jour à partir d'une source de mise à jour si celle-ci se trouve sur un segment différent du réseau et est identifiée par son adresse IPv6 avec lien local.

- Lorsque l'adresse IPv6 fait partie d'une URL, placez-la entre parenthèses.

- Pour les plages d'adresses IPv6, un préfixe et une longueur de préfixe sont généralement requis. Pour les configurations qui requièrent que le serveur interroge des adresses IP, des restrictions de longueur de préfixe s'appliquent afin d'empêcher tout problème de performance lorsque le serveur interroge un grand nombre d'adresses IP. Par exemple, pour la fonction de gestion des serveurs externes, la longueur du préfixe doit être comprise entre 112 (65,536 adresses IP) et 128 (2 adresses IP).
- Certains paramètres impliquant des adresses IPv6 ou des plages d'adresses IPv6 seront déployés pour les clients OfficeScan, mais ces clients OfficeScan n'en auront pas connaissance. Par exemple, si vous avez configuré la liste des sources Smart Protection et inclus un serveur Smart Protection Server identifié par son adresse IPv6, des clients OfficeScan avec une adresse IPv4 pure vont ignorer le serveur et se connecter à d'autres sources Smart Protection.

Écrans affichant les adresses IP

Cette rubrique dresse la liste des endroits de la console Web où sont affichées les adresses IP.

- Arborescence des clients

  Chaque fois que l'arborescence des clients s'affiche, les adresses IPv6 des clients OfficeScan IPv6 purs s'affichent dans la colonne **Adresse IP**. Les adresses IPv6 des clients OfficeScan à double pile s'affichent s'ils ont utilisé leur adresse IPv6 pour s'enregistrer sur le serveur.

  Remarque

  L'adresse IP utilisée par les clients OfficeScan à double pile lors de leur enregistrement sur le serveur peut être contrôlée dans **Ordinateurs en réseau** > **Gestion des clients > Adresse IP de votre choix**.

  Lorsque vous exportez les paramètres de l'arborescence des clients dans un fichier, les adresses IPv6 s'affichent également dans le fichier exporté.

- État du client

Les informations client détaillées sont disponibles lorsque vous accédez à **Ordinateurs en réseau** > **Gestion des clients > État**. Sur cet écran sont affichées les adresses IPv6 des clients OfficeScan IPv6 purs et des clients OfficeScan à double pile ayant utilisé leurs adresses IPv6 pour s'enregistrer sur le serveur.

- Journaux

  Les adresses IPv6 des clients OfficeScan à double pile et IPv6 purs apparaissent dans les journaux suivants :

  - Journaux de virus/programmes malveillants
  - Journaux de spywares/graywares
  - Journaux de pare-feu
  - Journaux de vérification de la connexion

- Console Control Manager

  Le tableau suivant répertorie les adresses IP du serveur OfficeScan et des clients OfficeScan s'affichant sur la console Control Manager.

TABLEAU A-3. Adresses IP du serveur OfficeScan et des clients OfficeScan s'affichant sur la console Control Manager

OFFICESCAN	VERSION DE CONTROL MANAGER		
	5.5 SP1	5.5	5.0
Serveur à double pile	IPv4 et IPv6	IPv4	IPv4
Serveur IPv4 pur	IPv4	IPv4	IPv4
Serveur IPv6 pur	IPv6	Non pris en charge	Non pris en charge
Client OfficeScan à double pile	Adresse IP utilisée lors de l'enregistrement du client OfficeScan sur le serveur OfficeScan	Adresse IP utilisée lors de l'enregistrement du client OfficeScan sur le serveur OfficeScan	Adresse IP utilisée lors de l'enregistrement du client OfficeScan sur le serveur OfficeScan

OfficeScan	Version de Control Manager		
	5.5 SP1	5.5	5.0
Client OfficeScan IPv4 pur	IPv4	IPv4	IPv4
Client OfficeScan IPv6 pur	IPv6	IPv6	IPv6

Annexe B

Prise en charge de Windows Server Core 2008

Cette annexe présente la prise en charge par OfficeScan de Windows Server Core 2008.

Prise en charge de Windows Server Core 2008

Windows Server Core 2008 est une installation minimale de Windows Server 2008. Dans un environnement Server Core :

- De nombreuses options et fonctionnalités de Windows Server 2008 sont supprimées.
- Le système exécute un système d'exploitation central beaucoup plus léger.
- Les tâches sont effectuées principalement depuis l'interface de ligne de commande.
- Le système d'exploitation exécute moins de services et nécessite moins de ressources au démarrage.

Le client OfficeScan prend en charge Server Core. Cette section contient des informations sur l'étendue de la prise en charge de Server Core.

Le serveur OfficeScan ne prend pas en charge Server Core.

Méthodes d'installation de Windows Server Core

Les méthodes d'installation suivantes ne sont pas prises en charge, ou le sont uniquement en partie :

- **Page Web d'installation :** Cette méthode n'est pas prise en charge car Server Core ne possède pas Internet Explorer.
- **Trend Micro Vulnerability Scanner :** L'outil Vulnerability Scanner ne peut être exécuté localement sur Server Core. Exécutez l'outil depuis le serveur OfficeScan ou un autre ordinateur.

Les méthodes d'installation suivantes sont prises en charge :

- Installation à distance. Pour obtenir des informations détaillées, voir *Installation à distance depuis OfficeScan Web Console à la page 4-18*.
- Configuration du script de connexion

- Client Packager

Installation du client OfficeScan à l'aide de l'outil de Configuration du script de connexion

Tâche

1. Ouvrez une invite de commande.
2. Mappez l'emplacement du fichier `AutoPcc.exe` en entrant la commande suivante :

   ```
   net use <lettre du lecteur mappé> \\< Nom d'hôte ou adresse IP du serveur OfficeScan>\ofcscan
   ```

   Par exemple :

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

   Un message s'affiche vous informant si l'emplacement du fichier AutoPcc.exe a été correctement mappé.
3. Accédez à l'emplacement du fichier `AutoPcc.exe` en indiquant la lettre du lecteur mappé suivie de deux points (:). Par exemple :

   ```
   P:
   ```
4. Entrez ce qui suit pour démarrer l'installation :

   ```
   AutoPcc.exe
   ```

L'écran ci-dessous montre les commandes et les résultats de l'invite de commande.

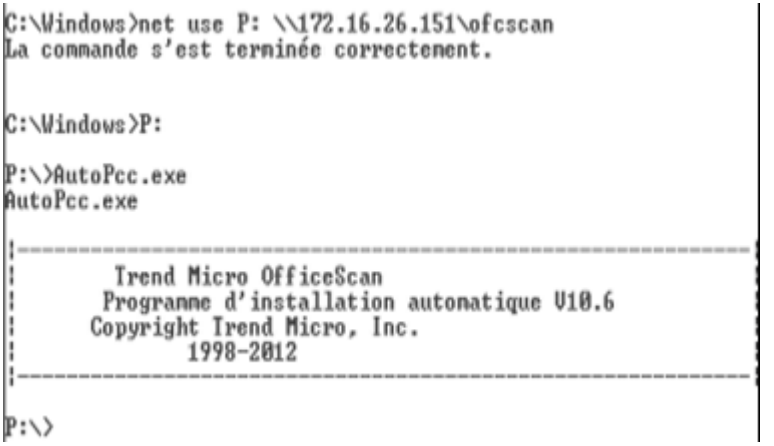


FIGURE B-1. Invite de commande indiquant comment installer le client OfficeScan à l'aide de la Configuration du script de connexion

Installation du client OfficeScan en utilisant à l'aide d'un pack client OfficeScan

Tâche

1. Créez le pack.

   Pour obtenir des informations détaillées, voir *Installation avec Client Packager à la page 4-23*.

2. Ouvrez une invite de commande.

3. Mappez l'emplacement du pack client OfficeScan en entrant la commande suivante :

   ```
   net use <lettre du lecteur mappé> \\<Emplacement du pack client>
   ```

   Par exemple :

```
net use P: \\10.1.1.1\Package
```

Un message vous informant si l'emplacement du pack client OfficeScan a été correctement mappé s'affiche.

4. Accédez à l'emplacement du pack client OfficeScan en indiquant la lettre du lecteur mappé suivie de deux points (:). Par exemple :

```
P:
```

5. Copiez le pack client OfficeScan dans un répertoire local de l'ordinateur Server Core en entrant la commande suivante :

```
copy <nom du fichier de pack> <répertoire de l'ordinateur Server Core où vous souhaitez copier le pack>
```

Par exemple :

```
copy officescan.msi C:\Client Package
```

Un message vous informant si le pack OfficeScan client a été correctement copié s'affiche.

6. Accédez au répertoire local. Par exemple :

```
C:
```

```
cd C:\Client Package
```

7. Entrez le nom du fichier de pack pour démarrer l'installation. Par exemple :

```
officescan.msi
```

L'écran ci-dessous montre les commandes et les résultats de l'invite de commande.

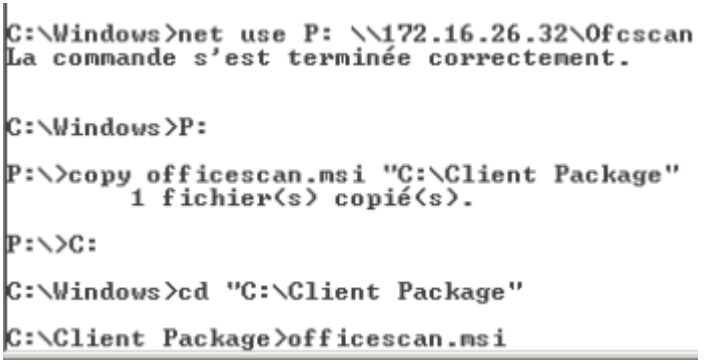


FIGURE B-2. Invite de commande indiquant comment installer le client OfficeScan à l'aide d'un pack client

Fonctionnalités du client OfficeScan sur Windows Server Core

La plupart des fonctionnalités du client OfficeScan disponibles sur Windows Server 2008 fonctionnent dans Server Core. La seule fonctionnalité non prise en charge est le mode itinérance.

Pour une liste des fonctionnalités disponibles sur Windows Server 2008, voir *Fonctionnalités du client OfficeScan à la page 4-3*.

La console du client OfficeScan n'est accessible que depuis l'interface de ligne de commande.

Remarque

Certains écrans de consoles client OfficeScan contiennent un bouton Aide. Lorsque l'on clique sur ce bouton, une aide HTML contextuelle s'ouvre. Étant donné que Windows Server Core 2008 ne contient pas de navigateur, ce type d'aide ne sera pas disponible. Pour y avoir accès, l'utilisateur doit installer un navigateur.

Commandes Windows Server Core

Lancez la console du client OfficeScan et d'autres tâches du client OfficeScan en saisissant des commandes dans l'interface de ligne de commande.

Pour exécuter les commandes, accédez à l'emplacement de `PccNTMon.exe`. Ce processus est responsable du lancement de la console du client OfficeScan. Vous le trouverez dans le <*Dossier d'installation du client*>.

Le tableau suivant répertorie les commandes disponibles.

TABLEAU B-1. Commandes Windows Server Core

COMMANDE	ACTION
`pccntmon`	Ouvre la console client OfficeScan
`pccnt`	
`pccnt <lecteur ou chemin d'accès du dossier>`	Effectue un scan du lecteur ou du dossier spécifié pour vérifier les risques de sécurité Directives : • Si le chemin d'accès du dossier contient un espace, mettez le chemin complet entre guillemets. • Il est impossible d'effectuer un scan de fichiers individuels. Commandes correctes : • `pccnt C:\` • `pccnt D:\Files` • `pccnt « C:\Documents and Settings »` Commandes incorrectes : • `pccnt C:\Documents and Settings` • `pccnt D:\Files\example.doc`
`pccntmon -r`	Ouvre la surveillance en temps réel
`pccntmon -v`	Ouvre une fenêtre contenant une liste des composants du client et de leur version

COMMANDE	ACTION
`pccntmon -u`	Ouvre une fenêtre dans laquelle vous pouvez lancer «Mettre à jour» (la mise à jour manuelle du client) Si «Mettre à jour» ne peut pas être lancé, le message suivant s'affiche dans l'invite de commande: Désactivé ou Non opérationnel
`pccntmon -n`	Ouvre une fenêtre contextuelle où est indiqué un mot de passe pour décharger le client Si aucun mot de passe n'est nécessaire pour décharger le client OfficeScan, le déchargement du client OfficeScan commence. Pour recharger le client OfficeScan, entrez la commande suivante : `pccntmon`
`pccntmon -m`	Ouvre une fenêtre contextuelle où est indiqué un mot de passe pour désinstaller le client OfficeScan Si aucun mot de passe n'est nécessaire pour désinstaller le client OfficeScan, la désinstallation du client OfficeScan.commence.

COMMANDE	ACTION

`pccntmon -c`	Affiche les informations suivantes dans la ligne de commande :
	• Méthode de scan
	  • Smart scan
	  • Scan traditionnel
	• État des signatures
	  • Mis à jour
	  • Obsolète
	• service de scan en temps réel
	  • Opérationnel
	  • Désactivé ou Non opérationnel
	• État de la connexion client
	  • En ligne
	  • Hors ligne
	• Services de réputation de sites Web
	  • Disponible
	  • Non disponible
	• Services de File Reputation
	  • Disponible
	  • Non disponible

`pccntmon -h`	Affiche toutes les commandes disponibles

Annexe C

glossaire

Les termes contenus dans ce glossaire fournissent des d'informations complémentaires sur les termes informatiques couramment référencés, ainsi que sur les produits et technologies Trend Micro.

ActiveUpdate

ActiveUpdate est une fonction commune à de nombreux produits Trend Micro. Connecté au site Web de mises à jour de Trend Micro, ActiveUpdate propose des téléchargements à jour de fichiers de signatures de virus, moteurs de scan, programmes et autres fichiers de composants Trend Micro via Internet.

Fichier compressé

Fichier unique contenant un ou plusieurs fichiers distincts ainsi que des informations leur permettant d'être extraits par un programme approprié, tel que WinZip.

Cookie

Mécanisme permettant de stocker des informations sur un utilisateur d'Internet, telles que son nom, ses préférences et ses centres d'intérêt, qui sont enregistrées dans le navigateur Web pour une utilisation ultérieure. La prochaine fois que vous accéderez à un site Web pour lequel votre navigateur dispose d'un cookie, le navigateur l'enverra au serveur Web et ce dernier pourra l'utiliser pour vous présenter des pages Web personnalisées. Par exemple, vous pouvez accéder à un site Web qui vous accueille en mentionnant votre nom.

Refus de service (DoS)

Le refus de service (DoS) est une attaque affectant un ordinateur ou un réseau et entraînant une perte du «service», c'est-à-dire de la connexion réseau. En général, les attaques de refus de service ont une incidence négative sur la bande passante du réseau ou surchargent les ressources de l'ordinateur telles que la mémoire.

DHCP

Dynamic Host Control Protocol (DHCP) est un protocole permettant d'affecter des adresses IP dynamiques aux dispositifs d'un réseau. Avec l'adressage dynamique, un dispositif peut avoir une adresse différente chaque fois qu'il se connecte au réseau. Sur certains systèmes, l'adresse IP du dispositif peut même changer alors qu'il est encore connecté. DHCP prend également en charge une combinaison d'adresses IP statiques et dynamiques.

DNS

Domain Name system (DNS) est un service à usage général d'interrogation de données servant principalement sur Internet à convertir les noms d'hôtes en adresses IP.

Lorsqu'un client DNS demande le nom d'hôte et les données d'adresse à un serveur DNS, le processus s'appelle résolution. Avec la configuration DNS de base, un serveur effectue une résolution par défaut. Par exemple, un serveur distant interroge un autre serveur pour obtenir les données figurant sur un ordinateur dans la zone actuelle. Le logiciel client du serveur distant interroge le résolveur, qui répond à la demande à partir de ses fichiers de base de données.

Nom de domaine

Nom complet d'un système, composé du nom d'hôte local et du nom de domaine correspondants, par exemple `tellsitall.com`. Un nom de domaine doit permettre de déterminer une adresse Internet unique pour tout hôte présent sur Internet. Ce processus, appelé « résolution de nom », utilise le système DNS (Domain Name System).

Adresse IP dynamique

Une adresse IP dynamique est une adresse IP attribuée par un serveur DHCP. L'adresse MAC de l'ordinateur reste la même ; toutefois, le serveur DHCP peut attribuer une nouvelle adresse IP à l'ordinateur, en fonction de la disponibilité.

ESMTP

ESMTP (Enhanced Simple Mail Transport Protocol) inclut la sécurité, l'authentification et d'autres dispositifs pour économiser la bande passante et protéger les serveurs.

Contrat de licence utilisateur final

Un contrat de licence utilisateur final ou CLUF est un contrat légal passé entre un éditeur de programme et l'utilisateur final. Il décrit généralement les restrictions s'appliquant à l'utilisateur, qui peut refuser de conclure l'accord en ne cliquant pas sur «J'accepte» au cours de l'installation. En cliquant sur «Je n'accepte pas», l'utilisateur mettra évidemment fin à l'installation du produit logiciel.

De nombreux utilisateurs acceptent par inadvertance d'installer un spyware et d'autres types de grayware sur leur ordinateur lorsqu'ils cliquent sur «J'accepte» sur des invites du CLUF s'affichant lors de l'installation de certains programmes gratuits.

Faux positif

On parle de faux positif lorsqu'un fichier est considéré à tort comme un fichier infecté par le logiciel de sécurité.

FTP

FTP (File Transfer Protocol) est un protocole standard utilisé pour transférer des fichiers d'un serveur vers un client via Internet. Consultez Network Working Group RFC 959 pour de plus amples informations.

GeneriClean

GeneriClean, programme aussi connu sous le nom de nettoyage référentiel, constitue une nouvelle technologie de nettoyage des virus/programmes malveillants qui ne nécessite pas de composants de nettoyage de virus. En utilisant un fichier détecté comme référence, GeneriClean détermine si le fichier détecté présente un processus/service correspondant dans la mémoire et une entrée de registre, puis supprime tous ces éléments.

Correctif de type hotfix

Un correctif de type Hot Fix désigne une solution palliative à un problème spécifique signalé par un utilisateur. Les correctifs de type hotfix sont spécifiques aux problèmes et ne sont dès lors pas proposés à tous les clients. Les correctifs de types hotfix Windows comprennent un programme d'installation. Ce n'est pas le cas des correctifs de types hotfix qui ne sont pas issus de Windows (en général, vous devez arrêter les démons du programme, copier le fichier pour écraser son équivalent dans votre installation, puis redémarrer les démons).

Par défaut, les clients OfficeScan peuvent installer des correctifs de type hotfix. Si vous ne voulez pas que les clients OfficeScan installent ce type de correctifs, modifiez les paramètres de mise à jour du client dans la console Web en accédant à **Ordinateurs en réseau** > **Paramètres clients généraux**, cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.

Si vous ne parvenez pas à déployer un correctif de type hotfix sur le serveur OfficeScan, utilisez Touch Tool pour changer l'horodatage du correctif de type hotfix. OfficeScan considère alors qu'il s'agit d'un nouveau correctif de type hotfix, ce qui amène le serveur à tenter automatiquement un nouveau déploiement du correctif. Pour plus de détails sur

cet outil, consultez *Exécution de l'outil Touch Tool pour les correctifs de type Hot Fix des clients OfficeScan à la page 5-54*.

HTTP

HTTP (Hypertext Transfer Protocol) est un protocole standard utilisé pour transférer des pages Web (y compris des graphiques et contenus multimédia) d'un serveur vers un client via Internet.

HTTPS

Protocole HTTP utilisant Secure Socket Layer (SSL). HTTPS est une variante de HTTP utilisée pour traiter les transactions sécurisées.

ICMP

Il arrive qu'une passerelle ou un hôte de destination utilise le protocole ICMP (Internet Control Message Protocol) pour communiquer avec un hôte source afin d'indiquer une erreur dans le traitement des datagrammes, par exemple. Le protocole ICMP utilise le support de base du protocole IP comme s'il s'agissait d'un protocole de niveau plus élevé ; cependant, le protocole ICMP fait en réalité partie intégrante du protocole IP et est implémenté par chaque module IP. Les messages ICMP sont envoyés dans les cas suivants : par exemple, lorsqu'un datagramme ne parvient pas à atteindre sa destination, lorsque la passerelle ne possède pas la capacité de tampon de transfert d'un datagramme et lorsque la passerelle peut diriger l'hôte afin d'acheminer le trafic via une route plus courte. Le protocole IP n'est pas conçu pour être parfaitement fiable. Le but de ces messages de contrôle est d'obtenir un retour d'informations concernant les problèmes dans l'environnement de communication, et non de rendre le protocole IP fiable.

IntelliScan

IntelliScan est une méthode d'identification des fichiers à scanner. Pour les fichiers exécutables (par exemple `.exe`), le véritable type du fichier est déterminé en fonction de

son contenu. Pour les fichiers non exécutables (au format `.txt` par exemple), le véritable type du fichier est déterminé en fonction de son en-tête.

IntelliScan offre les avantages suivants :

- Optimisation des performances : IntelliScan n'affecte pas les applications du client, car il exploite au minimum les ressources système de l'ordinateur.
- Durée de scan réduite : Comme IntelliScan est capable d'identifier le type réel des fichiers, il ne scanne que les fichiers réellement vulnérables aux infections. La durée du scan s'en trouve considérablement réduite, puisque tous les fichiers ne sont pas concernés.

IntelliTrap

Les auteurs de virus tentent souvent de contourner le filtrage antivirus en utilisant des algorithmes de compression en temps réel. IntelliTrap contribue à réduire les risques de telles incursions de virus sur le réseau en bloquant les fichiers exécutables compressés en temps réel et en les associant aux caractéristiques d'autres programmes malveillants. Étant donné qu'IntelliTrap identifie ces fichiers comme des risques de sécurité et peut bloquer malencontreusement des fichiers légitimes, Trend Micro vous recommande de mettre en quarantaine les fichiers (au lieu de les supprimer ou de les nettoyer) lorsque vous activez IntelliTrap. Si les utilisateurs échangent régulièrement des fichiers exécutables compressés en temps réel, désactivez IntelliTrap.

IntelliTrap utilise les composants suivants :

- Moteur de scan antivirus
- Signatures IntelliTrap
- Signatures d'exceptions IntelliTrap

IP

«Le protocole Internet (IP) permet de transmettre des blocs de données appelés datagrammes depuis l'emplacement source vers l'emplacement de destination, ces deux

emplacements étant des hôtes identifiés par des adresses de longueur définie.» (RFC 791)

Fichier Java

Java est un langage de programmation à usage général développé par Sun Microsystems. Un fichier Java contient du code Java. Java prend en charge la programmation sur Internet sous forme d'«applets» Java indépendantes des plates-formes. Une applet est un programme écrit en langage de programmation Java qui peut être inclus dans une page HTML. Lorsque vous utilisez un navigateur sur lequel la technologie Java est activée pour afficher une page contenant une applet, cette dernière transfère son code sur votre ordinateur et la machine virtuelle Java du navigateur l'exécute.

LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole applicatif permettant d'interroger et de modifier les services d'annuaire qui s'exécutent sur TCP/IP.

Port d'écoute

Un port d'écoute est utilisé pour les demandes de connexion client en vue d'un échange de données.

Agent MCP

Trend Micro Management Communication Protocol (MCP) constitue l'agent de nouvelle génération de Trend Micro pour les produits gérés. MCP remplace Trend Micro Management Infrastructure (TMI) comme Control Manager communique avec OfficeScan. MCP introduit plusieurs nouvelles fonctions :

- Chargement du réseau et taille de paquets réduits

- Prise en charge de la traversée des NAT et des pare-feux
- Prise en charge de HTTPS
- Prise en charge des communications bilatérale et unilatérale
- Prise en charge de l'authentification unique (Single sign-on ou SSO)
- Prise en charge des nœuds de cluster

Menaces combinées

Les menaces combinées tirent profit de plusieurs points d'accès et vulnérabilités dans les réseaux d'entreprise (menaces « Nimda » ou « Code Red », par exemple).

NAT

NAT (Network Address Translation) est une norme permettant de traduire les adresses IP sécurisées en adresses temporaires externes enregistrées provenant du pool d'adresses. Cette norme permet aux réseaux de confiance utilisant des adresses IP affectées de manière privée d'accéder à Internet. Cela évite également de devoir obtenir une adresse IP enregistrée pour chaque ordinateur du réseau.

NetBIOS

NetBIOS (Network Basic Input Output System) est une interface de programmation d'application (API) qui apporte des fonctionnalités, notamment en matière de réseau, au système BIOS (Basic Input/Output System) du DOS (Disk Operating System).

Communication unilatérale

La traversée des NAT est devenue un problème de plus en plus sérieux dans les environnements réseau actuels. Pour résoudre ce problème, le protocole MCP utilise

une communication unilatérale. La communication unilatérale fait en sorte que l'agent MCP lance la connexion vers le serveur et teste les commandes provenant du serveur. Chaque requête correspond à une demande de commande de type CGI ou à une transmission de journal. Pour réduire l'impact sur le réseau, l'agent MCP maintient la connexion autant que possible. Toute demande ultérieure utilise une connexion déjà ouverte. Si la connexion est interrompue, toutes les connexions SSL au même hôte bénéficient d'un cache d'ID de session réduisant de manière significative le temps de reconnexion.

Patch

Un patch désigne un groupe de hot fixes et de correctifs de sécurité qui résolvent plusieurs problèmes du programme. Trend Micro publie régulièrement des patchs. Les patchs Windows comprennent un programme d'installation alors que les patchs non issus de Windows disposent en général d'un script d'installation.

Attaque de phishing

Le phishing est une forme de fraude se développant rapidement qui vise à duper les internautes en reproduisant à l'identique l'apparence de sites Web légitimes afin de divulguer des informations personnelles.

On rencontre généralement le cas suivant : un utilisateur non averti reçoit un e-mail manifestement urgent (et ayant l'air authentique) lui notifiant un problème relatif à son compte qu'il doit résoudre immédiatement sous peine de fermeture du compte. Cet e-mail inclut une adresse URL dirigeant vers un site Web qui a tous les aspects du site original. Il est facile de copier l'e-mail et le site Web légitimes, puis de modifier le serveur principal où sont collectées les données envoyées.

Le message invite l'utilisateur à se connecter au site et à confirmer des informations sur le compte. Un pirate reçoit les données fournies par l'utilisateur, par exemple, un identifiant, un mot de passe, un numéro de carte de crédit ou de sécurité sociale.

Ce genre de fraude est rapide, peu onéreux et simple d'exécution. C'est une méthode également relativement rentable pour les criminels qui la pratiquent. Le phishing est

difficile à détecter même pour les utilisateurs avertis. Il en est de même pour les autorités judiciaires. Pire encore, il est quasiment impossible de poursuivre ses auteurs en justice.

Veuillez signaler à Trend Micro tout site Web susceptible de pratiquer des activités de phishing. Voir la *Envoi de fichiers suspects à Trend Micro à la page 17-27* pour plus d'informations.

Ping

Ping est un utilitaire qui envoie une requête d'écho ICMP à une adresse IP, puis attend la réponse. L'utilitaire Ping peut déterminer si l'ordinateur qui porte l'adresse IP spécifiée est connecté ou pas.

POP3

POP3 (Post Office Protocol 3) est un protocole standard pour le stockage et le transfert des messages depuis un serveur vers une application cliente de courrier électronique.

Serveur proxy

Un serveur proxy est un serveur Web acceptant les URL associées à un préfixe spécial, qui sert à extraire des documents d'une mémoire cache locale ou d'un serveur distant, puis renvoie l'URL au demandeur.

RPC

RPC (Remote Procedure Call) est un protocole réseau qui permet à un programme informatique s'exécutant sur un hôte de lancer l'exécution de code sur un autre hôte.

Correctif de sécurité

Un Patch de sécurité est centré sur les problèmes de sécurité pouvant être déployés sur tous les clients. Les patchs de sécurité Windows comprennent un programme d'installation alors que ceux qui ne sont pas issus de Windows disposent en général d'un script d'installation.

Service Pack

Un Service Pack désigne un regroupement de hot fixes, de correctifs et d'améliorations de fonctions suffisamment significatives pour être considérées comme une mise à niveau du produit. Les service packs Windows et non-Windows contiennent un programme et un script d'installation.

SMTP

SMTP (Simple Mail Transport Protocol) est un protocole standard utilisé pour acheminer les messages électroniques d'un serveur vers un autre et d'un ordinateur client vers un serveur via Internet.

SNMP

SNMP (Simple Network Management Protocol) est un protocole qui permet de surveiller les dispositifs connectés à un réseau afin de détecter les situations nécessitant une intervention de l'administrateur.

Déroutement SNMP

Un déroutement SNMP (Simple Network Management Protocol, protocole simple de gestion de réseau) est un procédé d'envoi de notifications aux administrateurs réseau qui utilisent des consoles d'administration prenant en charge ce protocole.

OfficeScan peut stocker les notifications dans les MIB (Management Information Bases ou bases d'informations d'administration). Vous pouvez utiliser les navigateurs MIB pour visualiser les notifications par déroutement SNMP.

Toutefois, OfficeScan ne tient à jour aucun fichier local MIB. Si Trend Micro Control Manager est installé, vous pouvez télécharger le fichier MIB de Control Manager et l'utiliser dans OfficeScan avec une application (par exemple HP™ OpenView) prenant en charge le protocole SNMP.

Pour utiliser le fichier MIB de Control Manager :

1. Accédez à la console d'administration de Control Manager.
2. Cliquez sur **Administration** dans le menu principal. Un menu déroulant apparaît.
3. Cliquez sur **Outils**.
4. Dans la zone de travail, cliquez sur **Fichier MIB de Control Manager**.
5. Dans l'écran Téléchargement de fichier, sélectionnez **Enregistrer**, indiquez un emplacement sur le serveur, puis cliquez sur **OK**.
6. Copiez le fichier sur le serveur OfficeScan, procédez à l'extraction du fichier MIB `cm2.mib` de Control Manager, fichier de base d'informations d'administration (Management Information Base ou MIB).
7. Importez le fichier `cm2.mib` à l'aide d'une application (par exemple HP OpenView) prenant en charge le protocole SNMP.

SOCKS°4

SOCKS 4 est un protocole TCP utilisé par les serveurs proxy pour établir une connexion entre les clients du réseau interne ou LAN et les ordinateurs ou serveurs externes au LAN. Le protocole SOCKS°4 soumet des demandes de connexion, établit des circuits proxy et relaie les données au niveau de la couche application du modèle OSI.

SSL

Protocole conçu par Netscape pour assurer la sécurité des données, constituant une couche entre les protocoles d'application (tels que HTTP, Telnet ou FTP) et TCP/IP. Ce protocole de sécurité assure le chiffrement des données, l'authentification du serveur, l'intégrité des messages et l'authentification éventuelle des clients pour une connexion TCP/IP.

Certificat SSL

Ce certificat numérique crée une communication HTTPS sécurisée.

TCP

TCP (Transmission Control Protocol) est un protocole de bout en bout fiable et orienté connexion conçu pour s'adapter à une hiérarchie de protocoles en couches prenant en charge des applications multiréseau. Le protocole TCP dépend des datagrammes IP pour la résolution des adresses. Consultez DARPA Internet Program RFC 793 pour de plus amples informations.

Telnet

Il s'agit d'une méthode standard de liaison entre des dispositifs terminaux via le protocole TCP grâce à la création d'un «terminal virtuel de réseau». Consultez Network Working Group RFC 854 pour de plus amples informations.

Port des chevaux de Troie

Les ports de chevaux de Troie sont couramment utilisés par les programmes de type cheval de Troie pour se connecter à un ordinateur. Lors d'une épidémie, OfficeScan bloque les numéros de port suivants, susceptibles d'être utilisés par les chevaux de Troie.

TABLEAU C-1. Ports des chevaux de Troie

NUMÉRO DE PORT	CHEVAL DE TROIE	NUMÉRO DE PORT	CHEVAL DE TROIE
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Port sécurisé

Le serveur et OfficeScan client utilisent des ports sécurisés pour communiquer.

Si vous bloquez les ports sécurisés, puis revenez aux paramètres réseau habituels après une épidémie, les OfficeScan clients ne rétabliront pas immédiatement la communication avec le serveur. La communication client-serveur ne sera rétablie qu'après écoulement du nombre d'heures que vous avez indiquées sur l'écran Paramètres de prévention des épidémies.

OfficeScan utilise le port HTTP (par défaut, 8080) comme port sécurisé sur le serveur. Lors de l'installation, il vous est possible de saisir un numéro de port différent. Pour bloquer ce port sécurisé ainsi que le port sécurisé sur OfficeScan client, vous devez cocher la case Bloquer les ports sécurisés sur l'écran Blocage des ports.

Le programme d'installation principal génère de façon aléatoire le port sécurisé de OfficeScan client pendant l'installation.

Détermination des ports sécurisés

Tâche

1. Accédez au <*dossier d'installation du serveur*>`\PCCSRV`.
2. Ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte comme le Bloc-notes.
3. Pour définir le port sécurisé du serveur, recherchez la chaîne «Master_DomainPort» et vérifiez la valeur figurant en regard de celle-ci.

   Par exemple, si la chaîne est la suivante : `Master_DomainPort=80`, cela signifie que le port 80 constitue le port sécurisé sur le serveur.
4. Pour définir le port sécurisé du client, recherchez la chaîne «Client_LocalServer_Port» et vérifiez la valeur figurant en regard de celle-ci.

   Par exemple, si la chaîne est la suivante : `Client_LocalServer_Port=41375`, cela signifie que le port 41375 constitue le port sécurisé sur le client.

Communication bilatérale

La communication bilatérale constitue une alternative à la communication unilatérale. Basée sur la communication unilatérale, mais disposant d'un canal HTTP supplémentaire recevant des notifications du serveur, la communication bilatérale permet d'améliorer l'envoi en temps réel et le traitement des commandes depuis le serveur par l'agent MCP.

UDP

UDP (User Datagram Protocol) est un protocole de communication sans connexion utilisé avec le protocole IP pour permettre aux programmes d'application d'envoyer des messages à d'autres programmes. Consultez DARPA Internet Program RFC 768 pour de plus amples informations.

Fichier non nettoyable

Le moteur de scan antivirus ne nettoie pas les fichiers suivants :

- Fichiers infectés par des chevaux de Troie
- Fichiers infectés par des vers
- Fichiers infectés protégés en écriture
- Fichiers protégés par mot de passe
- Fichiers de sauvegarde
- Fichiers infectés dans la corbeille
- Fichiers infectés dans le dossier Temp de Windows ou dans un dossier temporaire d'Internet Explorer

Fichiers infectés par des chevaux de Troie

Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement nuisibles, telles que l'affichage de messages, l'écrasement de

fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas.

Solution : OfficeScan utilise le moteur de nettoyage de virus et le modèle de nettoyage de virus pour supprimer les chevaux de Troie.

Fichiers infectés par des vers

Un ver informatique est un programme (ou ensemble de programmes) autonome qui peut répandre des copies fonctionnelles de lui-même ou de ses segments au sein d'autres systèmes informatiques. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome.

Solution : Trend Micro recommande de supprimer les vers.

Fichiers infectés protégés en écriture

Solution : Supprimez la protection en écriture pour autoriser OfficeScan à nettoyer le fichier.

Fichiers protégés par mot de passe

Comprennent les fichiers compressés protégés par mot de passe et les fichiers Microsoft Office protégés par mot de passe.

Solution : Supprimez la protection par mot de passe pour que OfficeScan puisse nettoyer ces fichiers.

Fichiers de sauvegarde

Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. OfficeScan crée une sauvegarde du fichier infecté au cas où le virus/programme malveillant l'endommagerait au cours du processus de nettoyage.

Solution : si OfficeScan a réussi à nettoyer le fichier infecté, vous n'avez pas besoin de conserver la copie de sauvegarde. Si l'ordinateur fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.

Fichiers infectés dans la corbeille

Lrsque le système fonctionne, OfficeScan risque de ne pas pouvoir supprimer les fichiers infectés placés dans la corbeille.

Solution basée sur le système d'exploitation :

Windows XP ou Windows Server 2003 avec le système de fichiers NTFS

Tâche

1. Connectez-vous sur l'ordinateur disposant des privilèges d'administrateur.
2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
3. Ouvrez l'invite de commande et saisissez ce qui suit afin d'effacer les fichiers:
   - `cd \`
   - `cd recycled`
   - `del *.* /S`
   - La dernière commande supprime tous les fichiers de la corbeille.
4. Vérifiez si les fichiers ont été supprimés.

Autres systèmes d'exploitation (ou ceux avec des systèmes de fichiers NTFS)

Tâche

1. redémarrez l'ordinateur en mode MS-DOS.
2. Ouvrez l'invite de commande et saisissez ce qui suit afin d'effacer les fichiers :
   - `cd \`
   - `cd recycled`
   - `del *.* /S`

- La dernière commande supprime tous les fichiers de la corbeille.

Fichiers infectés dans le dossier Temp de Windows ou dans un dossier temporaire d'Internet Explorer :

Il est possible que OfficeScan ne puisse pas nettoyer les fichiers infectés dans le dossier Temp de Windows ou dans le dossier temporaire d'Internet Explorer car l'ordinateur les utilise. Les fichiers à nettoyer sont peut-être des fichiers temporaires nécessaires au fonctionnement de Windows.

Solution basée sur le système d'exploitation :

Windows XP ou Windows Server 2003 avec le système de fichiers NTFS

Tâche

1. Connectez-vous sur l'ordinateur disposant des privilèges d'administrateur.
2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
3. Si le fichier infecté se trouve dans le dossier Temp de Windows:
   a. Ouvrez l'invite de commande et accédez au dossier Temp de Windows (situé par défaut sous `C:\Windows\Temp` sur les ordinateurs Windows XP ou Server 2003).
   b. Saisissez ce qui suit pour effacer les fichiers:

      ```
      cd temp

      attrib -h

      del *.* /S
      ```

      La dernière commande supprime tous les fichiers du dossier Temp de Windows.
4. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
   a. Ouvrez l'invite de commande et accédez au dossier temporaire d'Internet Explorer (situé par défaut sous `C:\Documents and Settings\<Votre`

`nom d'utilisateur>\Local Settings\Temporary Internet Files` pour les ordinateurs Windows XP ou Server 2003).

b. Saisissez ce qui suit pour effacer les fichiers:

```
cd tempor~1

attrib -h

del *.* /S
```

La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.

c. Vérifiez si les fichiers ont été supprimés.

Pour les ordinateurs exécutant d'autres systèmes d'exploitation (ou ceux sans NTFS) :

Tâche

1. redémarrez l'ordinateur en mode MS-DOS.

2. Si le fichier infecté se trouve dans le dossier Temp de Windows:

a. Lorsque l'invite de commande s'affiche, accédez au dossier Temp de Windows. Le dossier Temp de Windows par défaut sous Windows XP ou Server 2003 est `C:\Windows\Temp`.

b. Ouvrez l'invite de commande et saisissez ce qui suit afin d'effacer les fichiers:

```
cd temp

attrib -h

del *.* /S
```

La dernière commande supprime tous les fichiers du dossier Temp de Windows.

c. Redémarrez l'ordinateur en mode normal.

3. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:

a. Lorsque l'invite de commande s'affiche, accédez au dossier temporaire d'Internet Explorer. Le dossier temporaire d'Internet Explorer par défaut sous Windows XP ou Server 2003 est `C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary Internet Files`.

b. Entrez les commandes suivantes :

```
cd tempor~1

attrib -h

del *.* /S
```

La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.

c. Redémarrez l'ordinateur en mode normal.

Index

A

Access Control Server (ACS), 15-4
actions
    Prévention contre la perte de données, 9-45
actions de scan, 6-36
    spyware/grayware, 6-48
    virus/programmes malveillants, 6-72
action sur les événements système surveillés, 7-5
ActiveAction, 6-38
Active Directory, 2-27–2-30, 2-45, 2-50, 4-12, 4-30
    administration basée sur les rôles, 2-28
    étendue et requête, 13-72
    gestion des serveurs externes, 2-28
    Groupes de clients personnalisés, 2-28
    informations d'authentification, 2-29
    intégration, 2-27
    regroupement des clients, 2-45
    structure dupliquée, 2-50
    synchronisation, 2-30
ActiveSync, 9-44
administration basée sur les rôles, 2-28, 12-2
    comptes utilisateurs, 12-19
    rôles utilisateurs, 12-3
adresse IP de passerelle, 13-3
Adresse MAC, 13-3
Agent de mise à jour, 4-3, 4-28, 5-55
    attribution, 5-56
    configuration requise, 5-56
    duplication des composants, 5-62
    méthodes de mise à jour, 5-63
    rapport d'analyse, 5-63
    source de mise à jour standard, 5-58
Applications de messagerie instantanée, 9-35
arborescence client, 2-31–2-36, 2-39–2-42, 2-44
    affichages, 2-33
    à propos de, 2-31
    filtres, 2-33
    recherche avancée, 2-33, 2-34
    tâches générales, 2-32
    tâches spécifiques, 2-35, 2-36, 2-39–2-42, 2-44
        Déploiement de l'agent Cisco NAC, 2-44
        gestion des clients, 2-36
        Journaux de risques de sécurité, 2-42
        mises à jour des composants manuels, 2-40
        prévention des épidémies, 2-39
        rétrograder les mises à jour de composants, 2-41
ARP conflictuel, 11-4
assistance technique, 17-24
attaque LAND, 11-5
attaque par fragment minuscule, 11-5
attributs de fichier, 9-13, 9-18, 9-20
    caractères génériques, 9-20
    création, 9-20
    importation, 9-20
authentification, autorisation et mesure (AAA), 15-6
AutoPcc.exe, 4-10–4-12, 4-20, 4-21
autoprotection client, 13-13
Autorisations
    avancées, 8-11

nom et chemin d'accès du programme, 8-8
périphériques de stockage, 8-3
Périphériques qui ne sont pas destinés au stockage, 8-10
autorisations avancées
configuration, 8-11
périphériques de stockage, 8-5–8-7
autorité de certification (CA), 15-6

B

Base de connaissances, 17-25
blocage des ports, 6-105
Blocage du comportement des programmes malveillants, 7-2

C

Cache de signature numérique, 6-65
canaux réseau, 9-32, 9-33, 9-35–9-40
Applications de messagerie instantanée, 9-35
cibles contrôlées, 9-39, 9-40
cibles non contrôlées, 9-39, 9-40
clients de messagerie, 9-33
Étendue de transmission, 9-40
conflits, 9-40
toutes les transmissions, 9-37
transmissions externes, 9-38
étendue et cible de transmission, 9-37
FTP, 9-35
HTTP et HTTPS, 9-35
Protocole SMB, 9-36
webmail, 9-36
canaux système et application, 9-32, 9-40–9-42, 9-44
CD/DVD, 9-41
imprimante, 9-42
logiciel de synchronisation, 9-44
Peer To Peer (P2P), 9-42
Presse-papiers Windows, 9-44
stockage amovible, 9-42
canular, 6-2
caractères génériques, 9-20
attributs de fichier, 9-20
contrôle des dispositifs, 8-9
Case Diagnostic Tool, 17-2
Centre d'informations de sécurité, 17-26
certificat ACS, 15-19
certificat CA, 15-19, 15-21
certificats, 15-19
CA, 15-21
SSL, 15-38, 15-40
certificats numériques, 15-6
Certificat SSL, 15-38, 15-40
Certified Safe Software Service, 7-9
Check Point SecureClient, 4-29
cheval de Troie, 1-10, 5-6, 6-3
cibles contrôlées, 9-37, 9-39
cibles non contrôlées, 9-37, 9-39
Cisco NAC
architecture, 15-7
composants et terminologie, 15-3
déploiement du serveur Policy Server, 15-25
Cisco Trust Agent, 5-10, 15-4
Client Mover, 13-23
Client OfficeScan
clés de registre, 13-16
clients inactifs, 13-25
connexion au serveur Smart Protection Server, 13-42
connexion avec le serveur OfficeScan, 13-26, 13-41

désinstallation, 4-70
espace disque réservé, 5-49
fichiers, 13-15
importer et exporter des paramètres, 13-55
informations détaillées du client, 13-55
méthodes d'installation, 4-10
processus, 13-16
Client Packager, 4-12, 4-23, 4-24, 4-30, 4-31
déploiement, 4-25
paramètres, 4-26
clients, 2-45, 2-53–2-55, 3-30, 3-31, 4-2
connexion, 3-30
déplacement, 2-54
détection, 3-31
fonctions, 4-3
installation, 4-2
paramètres proxy, 3-30
regroupement, 2-45
suppression, 2-53
tri, 2-55
Clients inaccessibles, 13-45
clients inactifs, 13-25
clients itinérants, 4-6
code Java malveillant, 6-3
code malicieux ActiveX, 6-3
commentaires relatifs à la documentation, 17-27
composants, 2-19, 4-69, 5-2
privilèges et paramètres de mise à jour, 5-46
résumé des mises à jour, 5-64
sur l'agent de mise à jour, 5-55
sur le client, 5-27
sur le serveur OfficeScan, 5-15
Compression MSI, 4-12, 4-30, 4-31
comptes utilisateurs, 2-5
tableau de bord Résumé, 2-5
Configuration du script de connexion, 4-10–4-12, 4-20, 4-21
configuration requise
Agent de mise à jour, 5-56
Policy Server, 15-22
Conformité de la sécurité, 13-57
composants, 13-61
évaluations programmées, 13-70
gestion des serveurs externes, 2-28, 13-71
installation, 4-61
journaux, 17-9
mise en œuvre, 13-72
mise en œuvre des mises à jour, 5-53
paramètres, 13-64
scanner, 13-63
services, 13-59
console client
restriction d'accès, 13-18
console web, 1-9, 2-2–2-4
à propos de, 2-2
bannière, 2-4
compte de connexion, 2-3
configuration requise, 2-2
mot de passe, 2-3
URL, 2-3
contacter, 17-24–17-27
assistance technique, 17-24
Base de connaissances, 17-25
commentaires relatifs à la documentation, 17-27
envoi de fichiers suspects, 17-27
Trend Micro, 17-24–17-26
continuité de la protection, 3-11

contrat de licence utilisateur final (CLUF), C-4
Contrôle des actifs numériques
widgets, 2-22, 2-23
contrôle des dispositifs, 8-2, 8-3, 8-5–8-11, 8-13
Autorisations, 8-3, 8-5–8-8, 8-10
nom et chemin d'accès du programme, 8-8
autorisations avancées, 8-11
configuration, 8-11
caractères génériques, 8-9
configuration requise, 8-2
dispositifs externes, 8-10, 8-13
Fournisseur de Digital Signature, 8-8
gestion de l'accès, 8-10, 8-13
liste approuvée, 8-13
périphériques de stockage, 8-3, 8-5–8-7
Périphériques qui ne sont pas destinés au stockage, 8-10
Périphériques USB, 8-13
Contrôle des dispositifs, 1-11
journaux, 8-17, 17-10
notifications, 8-17
contrôle des dispositifs;liste de contrôle des dispositifs;liste de contrôle des dispositifs:ajout de programmes, 8-15
contrôle des performances, 6-30
Control Manager
intégration avec OfficeScan, 12-25
Journaux de l'agent MCP, 17-11
correctifs de type hotfix, 5-10, 5-54
critères
expressions personnalisées, 9-15
mots-clés, 9-23–9-25
critères d'épidémie, 6-99, 11-32
critères de scan
action des utilisateurs sur les fichiers, 6-27
compression de fichier, 6-28
fichiers à scanner, 6-27
programmation, 6-30
Utilisation de l'UC, 6-30

D

Damage Cleanup Services, 1-10, 4-4
déclarations de condition, 9-29
dépannage
Plug-in Manager, 14-10
désinstallation, 4-70
À partir de la console Web, 4-71
Plug-in Manager, 14-9
Protection des données, 9-66
utilisation du programme de désinstallation, 4-72
désinstallation du client, 4-70
détection, 3-31
d'emplacements, 3-31
détection d'emplacement, 13-2
détection des rootkits, 5-9
Digital Signature Pattern, 5-9, 6-65
dispositifs externes
gestion de l'accès, 8-10, 8-13
documentation, 2
domaines, 2-44, 2-45, 2-52–2-54
ajout, 2-52
regroupement des clients, 2-45
renommer, 2-54
suppression, 2-53
domaines de messagerie, 9-33
domaines de messagerie contrôlés, 9-33
domaines de messagerie non contrôlés, 9-33
DSP, 8-8
duplication des composants, 5-20, 5-62

E

éditeur SCV, 16-2
Encyclopédie des virus, 6-2
état de sécurité, 15-5
évaluations programmées, 13-70
événements du système surveillés, 7-3
exclusions de scan, 6-31
    extensions de fichier, 6-35
    fichiers, 6-34
    répertoires, 6-32
exporter des paramètres, 13-55
expressions, 9-13
    personnalisé, 9-14, 9-18
        critères, 9-15
    prédéfinies, 9-13, 9-14
expressions personnalisées, 9-14, 9-15, 9-18
    critères, 9-15
    importation, 9-18
Expressions prédéfinies, 9-13
    affichage, 9-14
Expressions rationnelles compatibles Perl (PCRE - Perl Compatible Regular Expressions), 9-14

F

FakeAV, 6-43
Fichier de signatures de virus, 5-3, 5-51, 5-53
fichier de signatures incrémentiel, 5-20
fichiers chiffrés, 6-44
fichiers compressés, 6-28, 6-70, 6-72
Fichiers de signatures
    Liste de blocage de sites Web, 3-9
    smart protection, 3-8
    Smart Scan Agent Pattern, 3-8
    Smart Scan Pattern, 3-9
fichiers suspects, 17-27
File Reputation, 3-3
Filtrage d'applications, 11-3
Fournisseur de Digital Signature, 8-8
    spécification, 8-8
Fragment de chevauchement, 11-5
Fragment trop important, 11-4
FTP, 9-35

G

Gateway Settings Importer, 13-5
gestion des serveurs externes, 2-28, 13-71
    demande programmée, 13-76
    journaux, 17-9
    résultats de la requête, 13-75
gestionnaire de quarantaine, 12-47
Groupes de clients personnalisés, 2-28, 2-45

H

HTTP et HTTPS, 9-35

I

Identificateurs de données, 9-13
    attributs de fichier, 9-13
    expressions, 9-13
    mots-clés, 9-13
IGMP fragmenté, 11-5
image disque client, 4-13, 4-36
importer des paramètres, 13-55
Informations sur le serveur Web, 12-45
installation, 4-2
    client, 4-2
    Conformité de la sécurité, 4-61
    Plugiciels, 14-5
    Plug-in Manager, 14-3
    Policy Server, 15-35
    Protection des données, 9-2
installation à distance, 4-11
installation du client, 4-2, 4-20

À partir de la console Web, 4-18
basé sur navigateur, 4-16
Client Packager, 4-23
Configuration du script de connexion, 4-20
configuration requise, 4-2
Depuis la page Web d'installation, 4-14
tâches après l'installation, 4-67
utilisation de l'image disque client, 4-36
utilisation de la Conformité de la sécurité, 4-61
utilisation de Vulnerability Scanner, 4-37
IntelliScan, 6-27
intranet, 3-13
IPv6, 3-23
Assistance, 3-23
IpXfer.exe, 13-23

J

jeton d'état, 15-5
journaux, 12-36
à propos de, 12-36
Journaux de contrôle des dispositifs, 8-17
journaux de mise à jour du client, 5-52
journaux de pare-feu, 11-25, 11-27, 11-30
journaux de réputation de sites Web, 10-11
journaux de restauration de spywares/graywares, 6-97
Journaux de risques de sécurité, 6-87
Journaux de scan, 6-97
journaux des événements du système, 12-35
journaux de spywares/graywares, 6-94
journaux de vérification de la connexion, 13-44
journaux de virus/programmes malveillants, 6-79, 6-87
Surveillance des comportements, 7-13
journaux de débogage
clients, 17-15
serveur, 17-3
journaux des clients
Journaux ActiveUpdate, 17-17
Journaux de connexion du client, 17-18
journaux de débogage, 17-15
Journaux de débogage de la prévention des épidémies, 17-18
Journaux de débogage de la réputation de sites Web, 17-21
Journaux de débogage de protection des données, 9-65, 17-22
Journaux de débogage du pare-feu OfficeScan, 17-19
Journaux de débogage TDI, 17-23
journaux de mise à jour du client, 17-18
Journaux de scan de courrier, 17-17
Journaux des mises à niveau/correctifs de type hotfix, 17-16
Journaux des nouvelles installations, 17-16
Journaux des services Damage Cleanup, 17-17
journaux du serveur
Journal de Client Packager, 17-8
Journaux Active Directory, 17-6
Journaux d'administration basée sur les rôles, 17-6
journaux d'installation/de mise à niveau à distance, 17-5
journaux d'installation/de mise à niveau locale, 17-5

Journaux de conformité de la sécurité, 17-9
Journaux de contrôle des dispositifs, 17-10
journaux de débogage, 17-3
Journaux de débogage de l'outil ServerProtect Migration, 17-10
Journaux de débogage de VSEncrypt, 17-11
Journaux de débogage du moteur de scan antivirus, 17-12
Journaux de gestion des serveurs externes, 17-9
Journaux de l'agent MCP de Control Manager, 17-11
journaux de mise à jour des composants, 17-7
Journaux de regroupement des clients, 17-7
journaux de réputation de sites Web, 17-10
Journaux de Virtual Desktop Support, 17-14
Journaux du serveur Apache, 17-8

L

licences, 12-40
état, 2-6
Protection des données, 9-4
liste approuvée, 6-49
Liste Certified Safe Software, 11-3
liste d'exceptions, 7-6
Surveillance des comportements, 7-6
Liste de blocage de sites Web, 3-9, 3-21
liste des programmes approuvés, 7-6
liste des programmes bloqués, 7-6
logiciel de sécurité tiers, 4-62
LogServer.exe, 17-3, 17-15

M

Mémoire cache du scan, 6-65
Mémoire cache du scan à la demande, 6-66
Menaces Internet, 10-2
méthode de scan, 4-26
par défaut, 6-8
méthodes de mise à jour
Agent de mise à jour, 5-63
clients, 5-37
Serveur OfficeScan, 5-25
Mettre à jour, 5-46
Microsoft SMS, 4-12, 4-31
migration
à partir d'un logiciel de sécurité tiers, 4-63
depuis des serveurs ServerProtect Normal, 4-64
mise à jour
Smart Protection Server, 5-14, 5-27
Mise à jour d'OfficeScan, 5-12
mise à jour du client
à partir du serveur ActiveUpdate, 5-47
automatique, 5-37
déclenchée par un événement, 5-38
manuelle, 5-44
mise à jour programmée, 5-39, 5-47
mise à jour programmée avec NAT, 5-42
privilèges, 5-46
source personnalisée, 5-31
Source standard, 5-30
mise à jour du serveur
duplication des composants, 5-20
journaux, 5-26
méthodes de mise à jour, 5-25

mise à jour manuelle, 5-25
mise à jour programmée, 5-26
paramètres proxy, 5-18
mise à niveau du client
désactiver, 5-47
mises à jour, 3-19, 3-20
Agent de mise à jour, 5-55
clients, 5-27
mise en œuvre, 5-53
Serveur OfficeScan, 5-15
Smart Protection Server intégré, 3-19, 3-20
mode d'évaluation, 6-75
Modèle de configuration de la surveillance des comportements, 5-9
Modèle de conformité aux stratégies, 5-9
Modèle de nettoyage de virus, 5-6
modèles, 9-27–9-31
déclarations de condition, 9-29
Opérateurs logiques, 9-29
personnalisé, 9-29–9-31
prédéfinies, 9-28
modèles personnalisés, 9-29
création, 9-30
importation, 9-31
modèles prédéfinis, 9-28
mot de passe, 12-46
Moteur de filtre URL, 5-8
Moteur de nettoyage de virus, 5-6
Moteur de scan anti-spyware, 5-7
Moteur de scan antivirus, 5-4
mots-clés, 9-13, 9-21
personnalisé, 9-23–9-25, 9-27
prédéfinies, 9-22
mots-clés personnalisés, 9-23
critères, 9-23–9-25
importation, 9-27
Mots-clés prédéfinis
distance, 9-22
nombre de mots-clés, 9-22

N

NetBIOS, 2-45
Network VirusWall Enforcer, 3-31
niveau de sécurité du client, 13-17
nombre d'entrées du journal du pare-feu, 11-27
notifications
Contrôle des dispositifs, 8-17
Détection des menaces Internet, 10-10
détection de spywares/graywares, 6-49
détection des virus/programmes malveillants, 6-44
épidémies, 6-99, 11-32
fichier de signatures de virus obsolète, 5-51
mise à jour du client, 5-51
pour les administrateurs, 9-56, 12-32
pour les utilisateurs clients, 6-83, 9-59
redémarrage de l'ordinateur, 5-52
violations du pare-feu, 11-28
nouvelles fonctionnalités, 1-2

O

OfficeScan
à propos de, 1-2
client, 1-13
composants, 2-19, 5-2
console web, 2-2
documentation, 2
Fonctionnalités et avantages principaux, 1-9
intégration SecureClient, 16-3

journaux, 12-36
licences, 12-40
mise à jour des composants, 4-69
programmes, 2-19
sauvegarde de la base de données, 12-43
scan de la base de données, 6-71
Serveur Web, 12-45
services du client, 13-12
terminologie, 4
onglets, 2-7
onglets prédéfinis, 2-10
Opérateurs logiques, 9-29
outil de génération de modèle de pré-scan VDI, 13-86
Outil Liste de dispositifs, 9-54
outil touch tool, 5-54

P

Page Web d'installation, 4-10, 4-14
Paramètres des services complémentaires, 13-6, 13-7
paramètres DHCP, 4-45
Paramètres du cache pour les scans, 6-65
paramètres proxy, 3-30
clients, 3-30
paramètres proxy automatiques, 13-53
pour la connexion externe, 13-51
pour la connexion interne, 13-50
pour la mise à jour des composants du serveur, 5-18
pour la réputation de sites Web, 10-9
privilèges, 13-52
pare-feu, 4-4, 11-2
avantages, 11-2
désactivation, 11-6
exceptions de stratégie, 11-14
exceptions de stratégie par défaut, 11-15
privilèges, 11-6, 11-24
profils, 11-4, 11-18
stratégies, 11-9
surveillance des épidémies, 11-6
tâches, 11-8
test, 11-34
patchs, 5-10
patchs de sécurité, 5-10
PCRE, 9-14
Performance Tuning Tool, 17-2
Périphérique d'accès au réseau, 15-4
périphériques de stockage
Autorisations, 8-3
autorisations avancées, 8-5–8-7
Périphériques qui ne sont pas destinés au stockage
Autorisations, 8-10
Périphériques USB
liste approuvée, 8-13
configuration, 8-13
phishing, C-10
Pilote de scan antivirus, 5-5
Pilote de surveillance des comportements, 5-9
Pilote du pare-feu commun, 5-7, 5-8, 17-19, 17-20
Ping of Death, 11-4
Plugiciels
installation, 14-5
Plug-in Manager, 1-9, 4-6, 14-2
dépannage, 14-10
désinstallation, 14-9
Gestion des fonctionnalités natives d'OfficeScan, 14-4
installation, 14-3
Policy Server pour Cisco NAC, 15-4

aperçu du déploiement, 15-25
certificat CA, 15-21
certificats, 15-19
certificat SSL, 15-19
configuration requise, 15-22
création des règles, 15-12
création des stratégies, 15-16
Installation de Policy Server, 15-35
processus de validation du client, 15-8
règles, 15-46
règles par défaut, 15-13, 15-14
stratégies, 15-46
stratégies et règles, 15-11
stratégies par défaut, 15-17
synchronisation, 15-47
Presse-papiers Windows, 9-44
Prévention contre la perte de données, 9-9–9-11, 9-13
actions, 9-45
attributs de fichier, 9-18, 9-20
Canaux:, 9-32
canaux réseau, 9-32, 9-33, 9-35–9-40
canaux système et application, 9-40–9-42, 9-44
expressions, 9-13–9-15, 9-18
Identificateurs de données, 9-13
modèles, 9-27–9-31
mots-clés, 9-21–9-25, 9-27
stratégie, 9-11
stratégies, 9-50
Prévention contre la perte de données:canaux système et application;canaux système et application;canaux système et application:chiffrement PGP, 9-42
Prévention contre la perte de données:règles de décompression;règles de décompression;fichiers compressés:règles de décompression, 9-45
prévention des épidémies, 2-17
désactivation, 6-108
stratégies, 6-104
Prise en charge d'IPv6, A-2
Affichage des adresses IPv6, A-7
Restrictions, A-3, A-4
privilèges
privilège de déchargement, 13-19
privilège de mode itinérance, 13-20
privilèges de configuration proxy, 13-52
privilèges de scan, 6-53
Privilèges de scan programmé, 6-56
privilèges du pare-feu, 11-24, 11-27
privilèges du scan de courrier, 6-62
privilèges de scan, 6-52
programmes, 2-19, 5-2
protection de périphérique externe, 5-9
Protection des données
déploiement, 9-6
désinstallation, 9-66
état, 9-9
installation, 9-2
licence, 9-4
Protocole SMB, 9-36
ptngrowth.ini, 3-18, 3-19

R

Rapport de conformité, 13-58
redémarrage du service, 13-12
Regroupement automatique de clients, 2-45, 2-47
regroupement des clients, 2-45–2-47, 2-49, 2-50, 2-52–2-55

Active Directory, 2-45, 2-49
Adresses IP, 2-50
ajout d'un domaine, 2-52
attribution d'un nouveau nom à un domaine, 2-54
automatique, 2-45, 2-47
déplacement d'un client, 2-54
DNS, 2-45
groupes personnalisés, 2-45
manuelle, 2-45, 2-46
méthodes, 2-45
NetBIOS, 2-45
suppression d'un domaine ou d'un client, 2-53
tâches, 2-52
tri des clients, 2-55
regroupement manuel des clients, 2-45, 2-46
Remote Authentication Dial-In User Service (RADIUS), 15-6
répertoire de quarantaine, 6-40, 6-45
réputation de sites Web, 1-11, 3-3, 3-4, 4-3, 10-2
journaux, 17-10
stratégies, 10-3
ressources de dépannage, 17-2
résumé
mises à jour, 5-64
tableau de bord, 2-5–2-7, 2-10
risques de sécurité, 6-2, 6-5, 6-7
attaques de phishing, C-10
protection contre, 1-10
spyware/grayware, 6-5, 6-7
rôle utilisateur
administrateur, 12-12
invité, 12-12
Trend Power User, 12-12

S

sauvegarde de la base de données, 12-43
scan anti-spywares/graywares
actions, 6-48
liste approuvée, 6-49
résultats, 6-95
scan antivirus/programmes malveillants
paramètres généraux, 6-69
résultats, 6-88
scan de la base de données, 6-71
scan de la messagerie, 4-6, 4-29, 6-62
scan de Microsoft Exchange Server, 6-72
scan des cookies, 6-76
scan de test, 4-69
Scan en temps réel, 6-15
Scan immédiat, 6-23
Scan manuel, 6-18
raccourci, 6-71
Scan programmé, 6-20
annuler et arrêter, 6-56, 6-78
arrêter automatiquement, 6-77
différer, 6-77
rappel, 6-77
reprendre, 6-78
scan traditionnel, 6-9, 6-10
passage à smart scan, 6-10
script de test EICAR, 4-69, 6-4
SDI, 11-4
SecureClient, 4-7, 16-2
éditeur SCV, 16-2
intégration à OfficeScan, 16-3
Serveurs Policy Server, 16-2
Secure Configuration Verification, 16-2
ServerProtect, 4-64
Server Tuner, 12-48
Serveur autonome, 3-7

serveur de référence, 12-30
serveur intégré, 3-7
Serveur OfficeScan, 1-12
    fonctions, 1-12
serveur Smart Protection Server autonome, 3-18
    ptngrowth.ini, 3-18
service de scan en temps réel, 13-40
Service principal de surveillance des comportements, 5-9
Signatures d'exceptions IntelliTrap, 5-6
Signatures de détection de l'analyse comportementale, 5-8
Signatures de spywares, 5-7
Signatures de surveillance active des spywares, 5-7
Signatures du pare-feu commun, 6-4
Signatures IntelliTrap, 5-6
Smart Feedback, 3-3
smart protection, 3-3, 3-4, 3-6–3-10, 3-13, 3-23
    environnement, 3-13
    Fichiers de signatures, 3-8–3-10
        Liste de blocage de sites Web, 3-9
        processus de mise à jour, 3-10
        Smart Scan Agent Pattern, 3-8
        Smart Scan Pattern, 3-9
    Services de File Reputation, 3-3
    Services de réputation de sites Web, 3-3, 3-4
    Smart Feedback, 3-3
    Smart Protection Network, 3-6
    Smart Protection Server, 3-7
    source, 3-7, 3-8
    sources, 3-23
        comparaison, 3-7
        détection, 3-23
        Prise en charge d'IPv6, 3-23
        protocoles, 3-8
    volume de menaces, 3-3
Smart Protection Network, 1-2, 3-6
Smart Protection Server, 3-7, 3-14, 3-18–3-21
    autonome, 3-7, 3-18
    installation, 3-14
    intégré, 3-7, 3-19–3-21
    mise à jour, 5-14, 5-27
    pratiques recommandées, 3-18
Smart Protection Server intégré, 3-19
    Liste de blocage de sites Web, 3-21
    mise à jour, 3-19, 3-20
        composants, 3-20
    ptngrowth.ini, 3-19
Smart Scan, 5-4, 6-9, 6-10
    passage du mode de scan traditionnel, 6-10
Smart Scan Agent Pattern, 3-8, 5-4
Smart Scan Pattern, 3-9, 5-4
source de mise à jour
    Agents de mise à jour, 5-58
    clients, 5-29
    Serveur OfficeScan, 5-17
spyware/grayware, 6-5, 6-7
    adware, 6-5
    applications de piratage des mots de passe, 6-5
    Canulars, 6-5
    menaces potentielles, 6-6
    numéroteur, 6-5
    outils d'accès à distance, 6-5
    outils de piratage, 6-5
    protection contre, 6-7
    restauration, 6-51
    spywares, 6-5

Statistiques du Top 10 des risques de sécurité, 2-17
stratégie, 9-11
stratégie de prévention des épidémies
    bloquer les ports, 6-105
    interdire l'accès en écriture, 6-107
    limitation/interdiction de l'accès aux dossiers partagés, 6-104
stratégies
    pare-feu, 11-4, 11-9
    Prévention contre la perte de données, 9-50
    réputation de sites Web, 10-3
Support Intelligence System, 2-5, 17-2
Surveillance des comportements, 7-13
    action sur les événements système, 7-5
    journaux, 7-13
    liste d'exceptions, 7-6
Surveillance des événements, 7-3
synchronisation, 15-47
SYN Flood, 11-5
Système de détection d'intrusion, 11-4

T

tableau de bord Résumé, 2-5–2-7, 2-10
    composants et programmes, 2-19
    comptes utilisateurs, 2-5
    état de la licence du produit, 2-6
    onglets, 2-7
    onglets prédéfinis, 2-10
    widgets, 2-7
    widgets prédéfinis, 2-10
tableaux de bord
    Résumé, 2-5–2-7, 2-10
tâches de préinstallation, 4-15, 4-18, 4-61
Teardrop, 11-5
Terminal Access Controller Access Control System (TACACS+), 15-6
TMPerftool, 17-2
TMTouch.exe, 5-54
TrendLabs, 17-26
Trend Micro
    Base de connaissances, 17-25
    Centre d'informations de sécurité, 17-26
    informations de contact, 17-24
    TrendLabs, 17-26
types de scan, 4-3, 6-14

U

Utilisation de l'UC, 6-30
utilitaire de compression, 6-4

V

validation du client, 15-5
variable de jeton, 6-102
VDI, 13-76
    journaux, 17-14
vérification de la connexion, 13-43
vers, 6-4
version d'évaluation, 12-40
Virtual Desktop Support, 13-76
virus/programmes malveillants, 6-2–6-4
    canular, 6-2
    cheval de Troie, 6-3
    code Java malveillant, 6-3
    code malicieux ActiveX, 6-3
    types, 6-2–6-4
    utilitaire de compression, 6-4
    vers, 6-4
    Virus/programmes malveillants probables, 6-2
    virus de macro, 6-3
    virus de test, 6-4

virus du secteur d'amorçage, 6-3
virus infectant les fichiers COM et EXE, 6-3
Virus VBScript, JavaScript ou HTML, 6-4
Virus/programmes malveillants probables, 6-2, 6-90
virus de macro, 6-3
virus de réseau, 6-3, 11-3
virus de test, 6-4
virus du secteur d'amorçage, 6-3
Virus HTML, 6-4
Virus infectant les fichiers COM, 6-3
Virus infectant les fichiers EXE, 6-3
virus JavaScript, 6-4
Virus VBScript, 6-4
Vulnerability Scanner, 4-13, 4-37
efficacité, 4-37
paramètres de ping, 4-58
paramètres DHCP, 4-45
protocoles pris en charge, 4-53
recherche de produits, 4-51
récupération de la description de l'ordinateur, 4-55

W

webmail, 9-36
widgets, 2-7, 2-11, 2-13, 2-16, 2-17, 2-19, 2-20, 2-22–2-26, 14-3
Carte des menaces de File Reputation, 2-26
Connectivité du client, 2-13
Contrôle des actifs numériques - Détections dans le temps, 2-23
Contrôle des actifs numériques - Détections en tête de liste, 2-22
Détection des risques liés à la sécurité, 2-16
disponible, 2-11
Épidémies, 2-17
Mashup d'OfficeScan et des plugiciels, 2-20
Mises à jour du client, 2-19
Sources majeures des menaces selon la réputation des sites Web, 2-24
Utilisateurs les plus menacés selon la réputation des sites Web, 2-25
widgets prédéfinis, 2-10
Windows Server Core, B-2
commandes, B-7
Fonctionnalités du client disponibles, B-6
Méthodes d'installation prises en charge, B-2